Version 4.0

PI's GUIDE TO INTERNATIONAL LAW AND SURVEILLANCE

March 2024

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters: our freedom to be human.

Open access. Some rights reserved.

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 4.0. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes.

You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence.

Privacy International is grateful to Creative Commons for its work and its approach to copyright. For more information please go to www.creativecommons.org.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321
privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

CONTENTS

About PI's guide to international law and surveillance *1*

Tips for users **2**

Section 1: The right to privacy in international and regional treaties *3*

Section 2: Surveillance and the right to privacy principles *6*

A. Affirmation of the principles underpinning the right to privacy **6**

B. The Principle of legality **17**

i. Accessibility requirement 38
ii. Foreseeability requirement 41

C. The Principle of necessity **54**

D. The Principle of proportionality **86**

E. The Principle of adequate safeguards **99**

i. Reasonable suspicion 108
ii. Judicial authorisation 111
iii. Effective oversight 132
iv. Data protection in surveillance 149
v. Transparency requirements 166
vi. Safeguards in intelligence sharing and data transfers 171
vii. Communications data (Metadata) 185
viii. Access to remedy: victimhood, standing, and notification 191
ix. duty to protect against third-party interference and access to remedy 219
x. Due diligence including impact assessments 220

Section 3: Safeguarding civic spaces *226*

a. Professional confidentiality and privileged communications –Legal professional privilege 227
b. Professional confidentiality and privileged communications – Protection of journalists' sources 236
c. Safety of journalists and human rights defenders 240
d. Protest surveillance 254

Section 4: Surveillance and other human rights provisions *271*

A. Surveillance and the jurisdictional clause (extraterritorial application) **271**

B. Surveillance and the principle of non-discrimination **276**

Section 5: Mass surveillance programmes *287*

Section 6: Surveillance-related capabilities *325*

A. Encryption and "Going Dark" **325**

B. The Debate over hacking, including spyware and vulnerability exploitation **335**

C. Biometric data processing in surveillance **343**

Section 6: The role and responsibilities of companies in surveillance *360*

Section 7: Acquiring and selling surveillance equipment *376*

List of sources *382*

ABOUT PI'S GUIDE TO INTERNATIONAL LAW AND SURVEILLANCE

The 21st century has brought with it rapid development in the technological capacities of governments and corporate entities to intercept, extract, filter, store, analyse, and disseminate the communications and data of whole populations. The costs of retaining data have decreased drastically and continue to do so every year. At the same time, the means of analysing the information have improved exponentially due to developments in automated machine learning and algorithmic design. These technological advancements pose a direct threat to the safeguards protecting the right to privacy, as well as other human rights.

Revelations about the scope and nature of digital surveillance around the world have led to a surge in legal discourse surrounding the role that international law, and in particular international human rights law, can and should play in responding to these practices. International bodies and regional human rights courts, international human rights treaty bodies and other human rights experts, such as UN special rapporteurs, have all published authoritative statements on the law strengthening the right to privacy in the sphere of surveillance in the 21st century.

First published in 2017, "PI's Guide to International Law and Surveillance" is an attempt to collate relevant excerpts from these judgments and reports into a single principled guide that will be regularly updated. This is the fourth edition of the Guide. It has been updated it to reflect the most relevant legal developments until March 2024.

The interpretation of the relevant international human rights framework has developed and expanded significantly since the Guide's initial publication in 2017. An ever-increasing number of resources provide more thorough reviews and insights on the impact that the digital era is

having on the right to privacy and other human rights. As a result, our understanding of the human rights standards that apply in surveillance is becoming more detailed and increasingly specialised. New entries on encryption, spyware, extraterritorial jurisdiction in surveillance, and facial recognition technologies reflect this evolution.

Despite its name, the Guide isn't just aimed at lawyers. It aspires to be a handy reference tool for anyone engaging in campaigning, advocacy, and scholarly research, on these issues. The Guide is meant to provide you with the most hard-hitting results that reinforce and strengthen the core principles and standards of international law on surveillance.

The guide is quite long. Here are a few useful tips to make the use of the Guide easier:

TIPS FOR USERS

- The Guide is not meant to be read it cover to cover;
- We suggest that you either use the table of contents or search for key words to find the most relevant quotes for you;
- In certain sections, you will find a brief explanatory note on the top clarifying the content therein and any connections with other sections;
- The quotes in each section appear in accordance with their source in chronological order, starting from the UN sources (i.e. resolutions, reports, concluding observations, individual complaints) and then looking into regional human rights systems;
- Certain quotes have been shortened to focus on the essence of the standards they provide. On occasion, it may be useful to go back to the original source;
- You can click on the number of any document to access the full document;
- Boxes across the guide highlight the most substantive articulation of the human rights standards applicable to the sub-issues covered under the relevant section. If you cite nothing else, these are the quotes that you want to reference;
- Only final judgments of the European Court of Human Rights are included.

Please reach out to us via email (info [@] privacyinternational [.] org) if you think there any additional references we should add, or topics you want us to cover.

SECTION 1: THE RIGHT TO PRIVACY IN INTERNATIONAL AND REGIONAL TREATIES

Universal Declaration of Human Rights (10 December 1948)

Article 12
No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

American Declaration on the Rights and Duties of Man (2 May 1948)

Article V
Every person has the right to the protection of the law against abusive attacks upon his honor, his reputation, and his private and family life.

European Convention for the Protection of Human Rights and Fundamental Freedoms (4 November 1950)

Article 8
(1) Everyone has the right to respect for his private and family life, his home and his correspondence.
(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

International Covenant on Civil and Political Rights (16 December 1966)

Article 17
(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
(2) Everyone has the right to the protection of the law against such interference or attacks.

American Convention on Human Rights (Pact of San Jose) (22 November 1969)

Article 11
(1) Everyone has the right to have his honor respected and his dignity recognized.
(2) No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
(3) Everyone has the right to the protection of the law against such interference or attacks.

Organization for Economic Cooperation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Part 1: General (23 September 1980)

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties [...]
6. These Guidelines should be regarded as minimum standards which can be supplemented by additional measures for the protection of privacy and individual liberties, which may impact

transborder flows of personal data.

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) (28 January 1981)

Article 1 – Object and Purpose
The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Convention on the Rights of the Child (20 November 1989)

Article 16
(1) No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation.
(2) The child has the right to the protection of the law against such interference or attacks.

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (18 December 1990)

Article 14
No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks.

Charter of Fundamental Rights of the European Union (7 December 2000)

Article 7
Everyone has the right to respect for his or her private and family life, home and communications.

Article 8
(1) Everyone has the right to the protection of personal data concerning him or her;
(2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified;
(3) Compliance with these rules shall be subject to control by an independent authority.

The Arab Charter on Human Rights (22 May 2004)

Article 16
Everyone charged with a criminal offence shall be presumed innocent until proved guilty by a final Judgment rendered according to law and, in the course of the investigation and trial, he shall enjoy the following minimum guarantees: … (8) The right to respect for his security of person and his privacy in all circumstances.

Article 21
(1) No one shall be subjected to arbitrary or unlawful interference with regard to his privacy, family, home or correspondence, nor to unlawful attacks on his honour or his reputation;
(2) Everyone has the right to the protection of the law against such interference or attacks.

Convention on the Rights of Persons with Disabilities (13 December 2006)

Article 22
(1) No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks.
(2) States Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others.

SECTION 2: SURVEILLANCE AND THE RIGHT TO PRIVACY PRINCIPLES

A. AFFIRMATION OF THE PRINCIPLES UNDERPINNING THE RIGHT TO PRIVACY

In this sub-chapter, you will find statements by different human rights bodies identifying and enumerating the fundamental principles that govern surveillance. These sources will mainly contain references to the need for surveillance to be in line with international human rights law more generally, or will specifically invoke the principles of legality, necessity, and proportionality.

These statements will often also refer to the importance of safeguards. Where this reference was made in combination with other principles, the statement has been included in this sub-chapter. Where they were referred to separately, such statements are located. In the introductory sub-chapter dedicated to safeguards.

Moreover, where re-statements of general principles were made in connection to specific forms of interference with the right to privacy (such as data collection and retention, or mass surveillance), references to these sources can be found in the sub-chapters dedicated to these notions in particular.

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

Recognizing the need to further discuss and analyse, based on international human rights law, issues relating to the promotion and protection of the right to privacy in the digital age, procedural safeguards, effective domestic oversight and remedies, the impact of surveillance on the right to privacy and other human rights, as well as the need to examine the principles of non-arbitrariness, lawfulness, legality, necessity and proportionality in relation to surveillance practices,

Emphasizing that unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data, hacking and the unlawful use of biometric technologies, as highly intrusive acts, violate the right to privacy, […], including when undertaken extraterritorially or on a mass scale,

Stressing also the need to ensure that national security and public health measures, including the use of technology to monitor and contain the spread of infectious diseases, are in full compliance with the obligations of States under international human rights law and adhere to the principles of lawfulness, legality, legitimacy with regard to the aim pursued, necessity and proportionality and the need to protect human rights, including the right to privacy, and personal data in the response to health or other emergencies,

4. *Recalls* that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality;

** See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016); UN*

General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014)

UN General Assembly Resolution on the Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc A/RES/72/180 (19 December 2017)

5. *Urges* States, while countering terrorism: (j) To review their procedures, practices and legislation regarding the surveillance and interception of communications and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law, and to take measures to ensure that interference with the right to privacy is regulated by law, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that such interference is not arbitrary or unlawful, bearing in mind what is reasonable for the pursuance of legitimate aims;

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

Recognizing the need to further discuss and analyse, on the basis of international human rights law, issues relating to the promotion and protection of the right to privacy in the digital age, procedural safeguards, effective domestic oversight and remedies and the impact of surveillance on the enjoyment of the right to privacy and other human rights, as well as the need to examine the principles of non-arbitrariness, lawfulness, legality, necessity and proportionality in relation to surveillance practices and to consider potential discriminatory effects, […]

Noting that the rapid pace of technological development enables individuals all over the world to use information and communications technology, and at the same time enhances the capacity of Governments, business enterprises and individuals to undertake surveillance, interception, hacking and data collection, which may violate or abuse human rights, in particular the right to privacy, and is therefore an issue of increasing concern, […]

2. *Recalls* that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality; […]

10. *Calls upon* States: (a) To respect and protect the right to privacy, including in the context of digital communications and new and emerging digital technologies;

(b) To take measures to end violations and abuses of the right to privacy and to create the conditions to prevent such violations and abuses, including by ensuring that relevant national legislation complies with their obligations under international human rights law, especially in the case of persons in vulnerable situations or marginalized groups;

(c) To review, on a regular basis, their procedures, practices and legislation regarding the surveillance of communications, including mass surveillance and the interception and collection of personal data, as well as regarding the use of profiling, automated decision-making, machine learning and biometric technologies, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(d) To respect international human rights obligations, including the right to privacy, when States intercept digital communications of individuals and/or collect personal data, when they share or otherwise provide access to data collected through, inter alia, information- and intelligence-sharing agreements and when they require disclosure of personal data from third parties, including business enterprises;

(e) To ensure that any measures taken to counter terrorism and violent extremism conducive to terrorism that interfere with the right to privacy are consistent with the principles of legality, necessity and proportionality and comply with their obligations under international law;

**See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/34/7 (23 March 2017); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/28/16 (26 March 2015)*

UN Human Rights Council Resolution on Terrorism and Human Rights, UN Doc A/HRC/RES/51/24 (7 October 2022)*

16. *Urges* all States to respect and protect the right to privacy, including in the context of digital communication, calls upon States, while countering terrorism and violent extremism conducive to terrorism, to review their procedures, practices and legislation regarding the surveillance of communications, their interception and collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law, and urges them to take measures to ensure that any interference with the right to privacy is regulated by law which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that such interference is consistent with the principles of legality, necessity and proportionality, and to comply with their obligations under international law;

**See also UN Human Rights Council Resolution on Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/HRC/RES/35/34 (23 June 2017)*

UN Human Rights Council Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, UN Doc A/HRC/RES/47/16 (7 July 2021)

Stressing the need to ensure that measures offline or online for the protection of national security, public order and public health are in full compliance with international law obligations and that the principles of lawfulness, legitimacy, necessity and proportionality are respected, and stressing also the need to protect human rights, including the freedom of opinion and expression, peaceful assembly and association and privacy, and personal data in the response to health or other emergencies,

Concluding Observations on Equatorial Guinea in the Absence of Its Initial Report, Human Rights Committee, UN Doc CCPR/C/GNQ/CO/1 (22 August 2019)

51. The State party should ensure: (a) that all types of surveillance activities and interference with privacy, including online surveillance for the purposes of State security, are governed by appropriate legislation that is in full accordance with the Covenant, in particular article 17, including with the principles of legality, proportionality and necessity, and that State practice conforms thereto;

UN General Assembly Resolution on the Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc A/RES/72/180 (19 December 2017)

5. *Urges* States, while countering terrorism: (i) To safeguard the right to privacy in accordance with international law, in particular international human rights law, and to take measures to ensure that interferences with or restrictions on that right are not arbitrary, are adequately regulated by law and are subject to effective oversight and appropriate redress, including through judicial review or other means;

UN Human Rights Council Resolution on Freedom of Opinion and Expression, UN Doc A/HRC/RES/50/15 (8 July 2022)

Stressing the need to ensure that measures for the respect of the rights or reputations of others and the protection of national security, public order and public health are in full compliance with international human rights obligations, including the principles of lawfulness, legitimacy, necessity and proportionality, and stressing also the need to protect human rights, including the right to freedom of opinion and expression and the right to privacy in accordance with obligations under international law, and safeguarding personal data,

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

51. Necessity and proportionality: while public surveillance may be permissible, States must demonstrate that measures are both necessary and proportionate. However, the effectiveness of surveillance measures is often doubtful, raising serious questions as to their necessity or proportionality.

56. […] OHCHR recommends that States: (a) Ensure that any interference with the right to privacy, including hacking, restrictions to access and use of encryption technology and surveillance of the public, complies with international human rights law, including the principles of legality, legitimate aim, necessity and proportionality and non-discrimination, and does not impair the essence of that right;

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

23. These authoritative sources [HRC General Comments 16, 27, 29, 31, and 34 and the Siracusa Principles] point to the overarching principles of legality, necessity and proportionality […] Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary.

Report of the Special Rapporteur on Contemporary Forms of Slavery, including its Causes and Consequences, UN Doc A/78/161 (12 July 2023)

41. […] Also, while the promotion of intelligence-led law enforcement with the use of surveillance and other technologies to identify the perpetrators and victims of contemporary forms of slavery may be reasonable, the collection of evidence on their criminal activities must also comply with existing international human rights standards, in particular those relating to the right to privacy. These include a clear legal basis, necessity, proportionality, robust independent oversight over law enforcement powers, as well as securing access to justice and remedies in case of a breach. […]

Report of the Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, The Guiding Principles on Business and Human Rights: Guidance on Ensuring Respect for Human Rights Defenders, UN Doc A/HRC/47/39/Add.2 (22 June 2021)

110. Illustrative actions that technology companies should take: As feasible, technology companies should avoid Internet shutdowns and geo-blocking; Commit to the confidentiality of digital communications, including encryption and anonymity; […] remind States that seek to use business enterprises to surveil individuals that this may only be conducted on a targeted basis, and only when there is reasonable suspicion that someone is engaging, or planning to engage, in serious criminal offences, based on principles of necessity and proportionality, and with judicial supervision […]

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/43/52 (24 March 2020)

52. States and non-State actors should: (b) Ensure that restrictions to the right to privacy, including through mass or targeted surveillance, requests for personal data or limitations on the use of encryption, pseudonymity and anonymity tools: (i) Are on a case-specific basis; (ii) Do not discriminate on the basis of gender or other factors, such as indigeneity; (iii) Are reasonable, necessary and proportionate as required by law for a legitimate purpose and ordered only by a court.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

50. As a primary step, Governments deploying surveillance tools must ensure that they do so in accordance with a domestic legal framework that meets the standards required by international human rights law. Surveillance should only be authorized in law for the most serious criminal offences. To be compliant with those standards, national laws must: (a) Emphasize that everyone enjoys the right not to be subjected to unlawful or arbitrary interference with his or her privacy and the right to hold opinions without interference and to seek, receive and impart information and ideas regardless of frontiers and through any media;

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/HRC/34/61 (21 February 2017)

36. The fact that surveillance powers are contained in public legislation is crucial to satisfying the principle of legality. The Special Rapporteur welcomes efforts by States to place intrusive surveillance regimes on a statutory footing, so that they can be subjected to public and parliamentary debate. However, publicly available primary legislation is not, in itself, sufficient to ensure the compatibility of those regimes with international human rights law. Necessity, proportionality and non-discrimination must also be taken into account along with the establishments of safeguards against arbitrariness, independent oversight and routes for redress.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/29/32 (22 May 2015)

31. Restrictions on encryption and anonymity, as enablers of the right to freedom of expression, must meet the well-known three-part test: any limitation on expression must be provided for by law; may only be imposed for legitimate grounds (as set out in article 19 (3) of the Covenant); and must conform to the strict tests of necessity and proportionality.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/20/17 (4 June 2012)

64. The Special Rapporteur reiterates that the right to freedom of expression should be fully

guaranteed online, as with offline content. If there is any limitation to the enjoyment of this right exercised through the internet, it must also conform to the criteria listed in article 19, paragraph 3, of the International Covenant on Civil and Political Rights. This means that any restriction imposed as an exceptional measure must (i) be provided by law, which is clear and accessible to everyone; (ii) pursue one of the legitimate purposes set out in article 19, paragraph 3, of the Covenant; and (iii) be proven as necessary and the least restrictive means required to achieved the purported aim.

Concluding Observations on the Fourth Periodic Report of Serbia, Human Rights Committee, UN Doc CCPR/C/SRB/CO/4 (26 March 2024)

37. The State party should ensure that draft legislation on the introduction of mass biometric surveillance is fully compatible with the Covenant, particularly article 17, […].

Concluding Observations on the Eighth Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/8 (26 March 2024)

51. […] [The State party] should ensure […] that its regulations relating to the intelligence-sharing of personal communications are in full conformity with the Covenant, in particular article 17, and that any interference with the right to privacy complies with the principles of legality, proportionality and necessity. […]

Concluding Observations on the Fifth Periodic Report of the Republic of Korea, Human Rights Committee, UN Doc CCPR/C/KOR/CO/5 (30 October 2023)

50. The State party should: (a) Ensure that all types of surveillance activities and interference with privacy – including online surveillance, interception of communications and communications data (metadata) and retrieval of data – are governed by appropriate legislation that is in full conformity with the Covenant, in particular with article 17 and the principles of legality, proportionality and necessity, and that State practice conforms thereto;

Concluding Observations on the Fifth Periodic Report of the United States of America, Human Rights Committee, UN Doc CCPR/C/USA/CO/5 (30 October 2023)

57. […] the State party should ensure that its surveillance activities, both within and outside its territory, conform to its obligations under the Covenant, including article 17, and that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under surveillance. It should adopt and effectively enforce, at all levels, through independent, impartial and well-resourced authorities, data privacy legislation for the public and private sectors that complies with international human rights law and includes safeguards, oversight and remedies to effectively protect the right to privacy. […]

**See also Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, UN Doc CCPR/C/USA/CO/4 (23 April 2014)*

Concluding Observations on the Fourth Periodic Report of the Islamic Republic of Iran, Human Rights Committee, UN Doc CCPR/C/IRN/CO/4 (26 October 2023)

46. The State party should amend the computer crimes law of 2010, the bill on a regulatory system for online services ("user protection bill") and the bill on supporting the family by promoting the culture of chastity and hijab, to ensure that any surveillance activity complies with the principles of legality, proportionality and necessity, in full conformity with the Covenant, in particular with articles 17 and 19 thereof. […]

Concluding Observations on the Second Periodic Report of Lesotho, UN Doc CCPR/C/LSO/CO/2 (21 July 2023)

50. The State party should: (a) Provide adequate human and financial resources for the operationalization of the Data Protection Commission so that it can effectively ensure the protection of the right to privacy in an independent manner; (b) Ensure that any surveillance activity complies with the principles of legality, proportionality and necessity, in full conformity with the Covenant, in particular article 17, and that surveillance activities are subject to effective judicial oversight mechanisms and ensure access to effective remedies in cases of abuse.

Concluding Observations on the Eighth Periodic Report of Colombia, UN Doc CCPR/C/COL/CO/8 (21 July 2023)

31. The State party should ensure that all types of surveillance, including online surveillance, and interference with privacy are in full compliance with article 17 of the Covenant, with full respect for the principles of legality, proportionality and necessity. […]

Concluding Observations on the Third Periodic Report of Brazil, Human Rights Committee, UN Doc CCPR/C/BRA/CO/3 (20 July 2023)

54. The State party should bring its legislation on data protection, facial recognition, surveillance activity and any interference with privacy into full conformity with the Covenant, in particular article 17, and with the principles of legality, proportionality, necessity and transparency, ensure its application and provide victims with access to effective remedies.

Concluding Observations on the Fourth Periodic Report of Zambia, Human Rights Committee, UN Doc CCPR/C/ZMB/CO/4 (20 March 2023)

32. The State party should review the Cyber Security and Cyber Crimes Act to ensure that any surveillance activities comply with the principles of legality, proportionality and necessity, in full conformity with the Covenant, in particular article 17 thereof. […]

Concluding Observations on the Seventh Periodic Report of Japan, Human Rights Committee, UN Doc CCPR/C/JPN/CO/7 (28 October 2022)

35. The State party should bring its regulations governing data retention and access, surveillance and interception activities into conformity with the Covenant, in particular article 17 thereof, and ensure strict adherence to the principles of legality, proportionality and necessity.

Concluding Observations on the Seventh Periodic Report of Germany, Human Rights Committee, UN Doc CCPR/C/DEU/CO/7 (11 November 2021)

43. The State party should ensure that all types of surveillance activities and interference with privacy are in full conformity with the Covenant, in particular article 17. Such activities should comply with the principles of legality, proportionality and necessity […]

Concluding Observations on Nigeria in the Absence of its Second Periodic Report, Human Rights Committee, UN Doc CCPR/C/NGA/CO/2 (29 August 2019)

41. The State party should (…) and take all necessary measures to ensure that all surveillance activities are in keeping with its obligations under article 17 of the Covenant and that any interference with the right to privacy is governed by law and conducted in accordance with the principles of necessity and proportionality and subject to effective safeguards.

Concluding Observations on the Third Periodic Report of Tajikistan, Human Rights

Committee, UN Doc CCPR/C/TJK/CO/3 (22 August 2019)

42. The State party should ensure that: (a) all types of surveillance activities and interference with privacy, including online surveillance, interception of communications and communications data (metadata) and retrieval of data, are governed by appropriate legislation that is in full conformity with the Covenant, in particular articles 17 and 19, including with the principles of legality, proportionality and necessity, and that State practice conforms thereto; (…)

Concluding Observations on the Fourth Periodic Report of Estonia, Human Rights Committee, UN Doc CCPR/C/EST/CO/4 (18 April 2019)

30. The State party should bring its regulations governing data retention and access thereto, surveillance and interception activities, and those relating to the intelligence-sharing of personal communications, into full conformity with the Covenant, in particular article 17, including with the principles of legality, proportionality and necessity. It should ensure that […] (b) access to communications data is limited to the extent strictly necessary for investigations into and prosecution of serious crimes;

Concluding Observations on the Fifth Periodic Report of Belarus, Human Rights Committee, UN Doc CCPR/C/BLR/CO/5 (22 November 2018)

44. The State party should ensure that: (a) all types of surveillance activities and interference with privacy, including online surveillance for the purposes of State security, are governed by appropriate legislation that is in full conformity with the Covenant, in particular article 17, including with the principles of legality, proportionality and necessity, and that State practice conforms thereto; […]

Concluding Observations on the Fourth Periodic Report of Bulgaria, Human Rights Committee, UN Doc CCPR/C/BGR/CO/4 (15 November 2018)

34. The State party should review its legislation in order to bring it into line with its obligations under the Covenant. It should, in particular: […] (c) Ensure that surveillance activities conform with its obligations under article 17 of the Covenant, including the principles of legality, necessity and proportionality, […]

Concluding Observations on the Third Periodic Report of Lebanon, Human Rights Committee, UN Doc CCPR/C/LBN/CO/3 (9 May 2018)

34. The State party should ensure that all laws governing surveillance activities, access to personal data and communications data (metadata) and any other interference with privacy are in full conformity with the Covenant, in particular article 17, including as regards the principles of legality, proportionality and necessity, and that State practice conforms thereto. […]

Concluding Observations on the Seventh Periodic Report of Norway, Human Rights Committee, UN Doc CCPR/C/NOR/CO/7 (25 April 2018)

21. The State party should take all the necessary steps to guarantee that its surveillance activities within and outside its territory are in conformity with its obligations under the Covenant, in particular article 17. Specifically, it should take measures to guarantee that any interference in a person's private life should be in conformity with the principles of legality, proportionality and necessity. It should ensure that the collection and use of data on communications take place on the basis of specific and legitimate objectives and that the exact circumstances in which such interference may be authorized and the categories of persons likely to be placed under surveillance are set out in detail in law. […]

Concluding Observations on the Second Periodic Report of Honduras, Human Rights

Committee, UN Doc CCPR/C/HND/CO/2 (27 July 2017) (translated from the original Spanish)

39. The State party should take all necessary measures to ensure that its monitoring activities are in line with its obligations under the Covenant, especially Article 17, and that any interference with the right to privacy is in accordance with the principles of legality, necessity and proportionality [...]

Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, UN Doc CCPR/C/ITA/CO/6 (28 March 2017)

37. The State party should review the regime regulating the interception of personal communications, hacking of digital devices and the retention of communications data with a view to ensuring (a) that such activities conform with its obligations under article 17 including with the principles of legality, proportionality and necessity,

Concluding Observations on the Second Periodic Report of Turkmenistan, Human Rights Committee, UN Doc CCPR/C/TKM/CO/2 (28 March 2017)

37. The State party should ensure that: (a) all types of surveillance activities and interference with privacy, including online surveillance for the purposes of State security, are governed by appropriate legislation that is in full conformity with the Covenant, in particular article 17, including with the principles of legality, proportionality and necessity, and that State practice conforms thereto.

Concluding Observations on the Seventh Periodic Report of Colombia, Human Rights Committee, UN Doc CCPR/C/COL/CO/7 (4 November 2016)

33. The State party should: […] (c) Take the necessary steps to ensure that any interference with a person's privacy, including interference via the electromagnetic spectrum, is in keeping with the principles of legality, necessity and proportionality; (d) Ensure that the implementation of laws governing matters that could have repercussions on the enjoyment of the right to privacy, in particular Act No. 1621 and the new Police Code, is entirely in keeping with the State party's obligations under the Covenant and, in particular, its obligations under article 17.

Concluding Observations on the Sixth Periodic Report of Morocco, Human Rights Committee, UN Doc CCPR/C/MAR/CO/6 (4 November 2016)

38. The State party should take all necessary steps to ensure that its surveillance activities are in keeping with its obligations under the Covenant, including article 17, and ensure that any breach of privacy is in keeping with the principles of legality, proportionality and necessity. […]

Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee, UN Doc CCPR/C/POL/CO/7 (4 November 2016)

39. The Committee is concerned about the surveillance and interception powers of the Polish intelligence and law enforcement authorities as reflected in the Law on Counterterrorism of June 2016 and the Act amending the Police Act and certain other acts of January 2016. The Committee is particularly concerned about: a) the unlimited and indiscriminate surveillance of communications and collection of metadata b) the targeting of foreign nationals and application of different legal criteria to them, […].

40. The State party should review its counterterrorism legislation in order to bring it into line with its obligations under the Covenant, and ensure that any interference with the right to privacy complies with the principles of legality, necessity and proportionality."

Concluding Observations on the Sixth Periodic Report of Denmark, Human Rights Committee, UN Doc CCPR/C/DNK/CO/6 (15 August 2016)

28. The State party should clearly define the acts that constitute terrorism in order to avoid abuses. The State party should ensure that the application of such legislation is compliant with the Covenant and that the principles of necessity, proportionality and non-discrimination are strictly observed.

Concluding Observations on the Fourth Periodic Report of Rwanda, Human Rights Committee, UN Doc CCPR/C/RWA/CO/4 (2 May 2016)

36. The State party should take legislative and other measures necessary to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity. […]

Concluding Observations on the Initial Report of South Africa, Human Rights Committee, UN Doc CCPR/C/ZAF/CO/1 (27 April 2016)

43. The State party should take all measures necessary to ensure that its surveillance activities conform to its obligations under the Covenant, including article 17, and that any interference with the right to privacy complies with the principles of legality, necessity and proportionality... […]

Concluding Observations on the Third Periodic Report of the Former Yugoslav Republic of Macedonia, Human Rights Committee, UN Doc CCPR/C/MKD/CO/3 (17 August 2015)

23. The State party should take all measures necessary to ensure that its surveillance activities conform to its obligations under the Covenant, including article 17. In particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity."

Concluding Observations on the Fifth Periodic Report of France, Human Rights Committee, UN Doc CCPR/C/FRA/CO/5 (17 August 2015)

12. [...] Specifically, measures should be taken to guarantee that any interference in persons' private lives should be in conformity with the principles of legality, proportionality and necessity. […]

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/7 (17 August 2015)*

24. […] measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance.

***Škoberne v Slovenia*, App No 19920/20, Judgment, European Court of Human Rights (15 February 2024)**

120. Any interference with an individual's Article 8 rights can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which that paragraph refers and is necessary in a democratic society in order to achieve any such aim (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 227, ECHR 2015, and *Kennedy v. the United Kingdom*, no. 26839/05, § 130, 18 May 2010). […]

***Potoczká and Adamčo v Slovakia*, App No 7286/16, Judgment, European Court of Human Rights (12 January 2023)**

69. The Court reiterates that (i) telephone conversations are covered by the notions of "private life" and "correspondence" within the meaning of Article 8, (ii) their monitoring amounts to an interference

with the exercise of the rights under Article 8, and (iii) such interference is justified by the terms of paragraph 2 of Article 8 only if it is "in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 and is "necessary in a democratic society" in order to achieve the aim or aims (see, among many other authorities, *Dragojević*, cited above, §§ 78-79, with further references).

***Nuh Uzun and Others v Türkiye*, App No 49341/18 and 13 others, Judgment, European Court of Human Rights (29 March 2022) (translated from the original French)**

83. The Court emphasises that, in order not to infringe Article 8 of the Convention, such interference must have been "prescribed by law", pursue a legitimate aim within the meaning of paragraph 2 and, moreover, be necessary in a democratic society in order to achieve that aim (see, among many other authorities, *Rotaru v. Romania* [GC], no. 28341/95, § 48, ECHR 2000 V).

***Escher et al. v Brazil*, Inter-American Court of Human Rights, Judgment (on Preliminary Objections, Merits, Reparations, and Costs) Series C No 200 (6 July 2009)**

129. Since the telephone conversations of the alleged victims were private and they had not authorized that their conversations be conveyed to third parties, the interception of the conversations by State agents constituted interference in their private life. Therefore, the Court must examine whether this interference was arbitrary or abusive in the terms of Article 11(2) of the Convention or whether it was compatible with the said treaty. As indicated previously (supra para. 116), to conform to the American Convention any interference must comply with the following requirements: (a) it must be established by law; (b) it must have a legitimate purpose, and (c) it must be appropriate, necessary and proportionate. Consequently, the absence of any of these requirements implies that the interference is contrary to the Convention […]

African Commission on Human and Peoples' Rights, Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa, ACHPR/Res.573 (LXXVII) (9 November 2023)

The African Commission calls on States Parties to: i. Ensure that all restrictions on the rights to privacy and other fundamental freedoms, such as freedom of expression, freedom of association and freedom of assembly, are necessary and proportionate, and in line with the provisions of international human rights law and standards.

***NG v Direktor na Glavna direktsia 'Natsionalna politsia' pri Ministerstvo na vatreshnite raboti – Sofia* (C-118/22), Judgment, Grand Chamber, Court of Justice of the European Union (30 January 2024)**

39 In the first place, it should be borne in mind that the fundamental rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society and be weighed against other fundamental rights. Any limitation on the exercise of those fundamental rights must, in accordance with Article 52(1) of the Charter, be provided for by law, respect the essence of those fundamental rights and observe the principle of proportionality. Under the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. They must apply only in so far as is strictly necessary and the legislation which entails the limitations in question must lay down clear and precise rules governing the scope and application of those limitations (see, to that effect, judgment of 22 June 2021, Latvijas Republikas Saeima (Penalty points), C-439/19, EU:C:2021:504, paragraph 105 and the case-law cited).

B. THE PRINCIPLE OF LEGALITY

The following sub-chapter is structured as follows: where human rights mechanisms refer to the principle of legality in general and explain the qualities that the legal basis must possess, the quote may be found in the introduction of the principle. These statements will often include more general references to the requirements of accessibility and foreseeability. Where the statement is a reference to these requirements but not a more detailed explanation of their content, the reference is included in the introduction of the principle. Where these principles are explained separately from one another, the references are included in the relevant sub-chapters.

The review of pronouncements by different human rights monitoring mechanisms shows that there are significant overlaps in references to the principles of legality, necessity and proportionality. Whether an appraisal is made within the test of necessity or proportionality will also often depend on the particular approach adopted by the court in question. This is particularly the case for the principles of necessity and proportionality, as well as whether the aim pursued is an element in the assessment of necessity, or of legality. It may therefore be pertinent to also consult other sub-chapters. Reference to the principle of legality within the broader framework of principles governing surveillance can be found in the introductory sub-chapter A.

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

Noting in particular that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that any interference with the right to privacy must not be arbitrary or unlawful, bearing in mind what is reasonable with regard to the pursuance of legitimate aims, and recalling that States that are parties to the International Covenant on Civil and Political Rights must take the necessary steps to adopt laws or other measures as may be necessary to give effect to the rights recognized in the Covenant.

**See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014)*

UN General Assembly Resolution on the Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc A/RES/72/180 (19 December 2017)

5. *Urges* States, while countering terrorism:

(j) To review their procedures, practices and legislation regarding the surveillance and interception of communications and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law, and to take measures to ensure that interference with the right to privacy is regulated by law, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that such

interference is not arbitrary or unlawful, bearing in mind what is reasonable for the pursuance of legitimate aims;

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

Noting in particular that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that any interference with the right to privacy must be consistent with the principles of legality, necessity and proportionality, bearing in mind what is reasonable with regard to the pursuance of legitimate aims, and recalling that States that are parties to the International Covenant on Civil and Political Rights must take the steps necessary to adopt laws or other measures as may be necessary to give effect to the rights recognized in the Covenant, […]

9. *Calls upon* all States: (c) To review, on a regular basis, their procedures, practices and legislation regarding the surveillance of communications, including mass surveillance and the interception and collection of personal data, as well as regarding the use of profiling, automated decision-making, machine learning and biometric technologies, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

* See also *UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021)*

UN Human Rights Council Resolution on Terrorism and Human Rights, UN Doc A/HRC/RES/51/24 (7 October 2022)

16. *Urges* all States […] to take measures to ensure that any interference with the right to privacy is regulated by law, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, […];

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

35. The law must be publicly accessible. Secret rules and secret interpretations of law do not have the necessary qualities of "law" (ibid., para. 29). Laws need to be sufficiently precise. Discretion granted to the executive or a judge and how such discretion may be exercised must be circumscribed with reasonable clarity (see A/69/397, para. 35). To that end, the nature of the offence and the category of persons that may be subjected to surveillance must be described. Vague and overbroad justifications, such as unspecific references to "national security" do not qualify as adequately clear laws. Surveillance must be based on reasonable suspicion and any decision authorizing such surveillance must be sufficiently targeted. The law must strictly assign the competences to conduct surveillance and access the product of surveillance to specified authorities.

36. In terms of its scope, the legal framework for surveillance should cover State requests to business enterprises. It should also cover access to information held extraterritorially or information-sharing with other States. A structure to ensure accountability and transparency within governmental organizations carrying out surveillance needs to be clearly established in the law.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

24. […] (a) Provided by law/legality: any restriction must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. Any restriction may not be unduly vague or overbroad such that it could confer unfettered discretion on officials […].

25. […] surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory.

50. As a primary step, Governments deploying surveillance tools must ensure that they do so in accordance with a domestic legal framework that meets the standards required by international human rights law. Surveillance should only be authorized in law for the most serious criminal offences. […]

Concluding Observations on the Second Periodic Report of Botswana, Human Rights Committee, UN Doc CCPR/C/BWA/CO/2 (11 November 2021)

31. The State party should ensure that: (a) All types of surveillance activities and interference with privacy, including online surveillance, interception of communications, access to communications data and retrieval of data, are governed by appropriate legislation that conforms with the Covenant, in particular article 17, including with the principles of legality, proportionality and necessity;

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet, OEA/Ser.L/V/II. CIDH/RELE/INF.11/13 (31 December 2013)

153. [...] the limitations on [the right to privacy and associated rights] must be established beforehand in a law, and set forth expressly, exhaustively, precisely, and clearly, both substantively and procedurally. This means that there must be a law that results from the deliberation of a legislative body, which precisely defines the causes and conditions that would enable the State to intercept the communications of individuals, collect communications data or "metadata," or to subject them to surveillance or monitoring that invades spheres in which they have reasonable expectations of privacy."

154. As this Office of the Special Rapporteur has already indicated, clandestine espionage conducted unlawfully or without legal support is an act that is highly offensive to fundamental rights and seriously compromises the actions of the State, its international responsibility, and even the very basis of democracy.

UN General Assembly Resolution on the United Nations Global Counter-Terrorism Strategy: eighth review, UN Doc A/RES/77/298 (22 June 2023)*

107. *Calls upon* States, while countering terrorism and preventing violent extremism conducive to terrorism, to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, by ensuring the full and effective implementation of all their obligations under international human rights law;

** See also UN General Assembly Resolution on The United Nations Global Counter-Terrorism Strategy: Seventh Review, UN Doc A/RES/75/291 (30 June 2021)*

UN General Assembly Resolution on Terrorism and Human Rights, UN Doc A/RES/78/210 (19 December 2023)*

30. *Urges* States to safeguard the right to privacy in accordance with international law, in particular international human rights law, and to take measures to ensure that interference with or restriction of that right are not arbitrary, are adequately regulated by law and are subject to effective oversight and appropriate redress, including through judicial review or other means;

**See also UN General Assembly Resolution on Terrorism and Human Rights, UN Doc A/RES/74/147 (18 December 2019); UN General Assembly Resolution on Terrorism and Human Rights, UN Doc A/RES/73/174 (17 December 2018)*

UN Human Rights Council Resolution on Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/HRC/RES/35/34 (23 June 2017)

20. *Urges* all States to respect and protect the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, including in the context of digital communication, and calls upon States, while countering terrorism and violent extremism conducive to terrorism, to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law, and *urges* them to take measures to ensure that any interference with the right to privacy is regulated by law, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that such interference is not arbitrary or unlawful, bearing in mind what is reasonable to the pursuance of legitimate aims;

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

49. Legality: […] dedicated legal instruments are required, in particular for surveillance done in the context of law enforcement and national security. Laws and regulations need to have clearly determined and strict limitations on the access and merging of government databases. […]
57. […] OHCHR recommends that States: (c) Adopt adequate legal frameworks that govern the collection, analysis and sharing of social media intelligence that clearly define permissible grounds, prerequisites, authorization procedures and adequate oversight mechanisms;

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

23. Any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear, and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances...

28. The State must ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/29/32 (22 May 2015)

31. Restrictions on encryption and anonymity, as enablers of the right to freedom of expression, must meet the well-known three-part test: any limitation on expression must be provided for by law; may only be imposed for legitimate grounds (as set out in article 19 (3) of the Covenant); and must conform to the strict tests of necessity and proportionality.

32. First, for a restriction on encryption or anonymity to be "provided for by law", it must be precise, public and transparent, and avoid providing State authorities with unbounded discretion to apply the. Proposals to impose restrictions on encryption or anonymity should be subject to public comment and only be adopted, if at all, according to regular legislative process. Strong procedural and judicial safeguards should also be applied to guarantee the due process rights of any individual whose use of encryption or anonymity is subject to restriction. In particular, a court, tribunal or other independent adjudicatory body must supervise the application of the restriction.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014)

35. Article 17 of the Covenant explicitly provides that everyone has the right to the protection of the law against unlawful or arbitrary interference with their privacy. This imports a "quality of law" requirement that imposes three conditions: (a) the measure must have some basis in domestic law; (b) the domestic law itself must be compatible with the rule of law and the requirements of the Covenant; and (c) the relevant provisions of domestic law must be accessible, clear and precise.

Concluding Observations on the Third Periodic Report of Turkmenistan, UN Doc CCPR/C/TKM/CO/3 (17 March 2023)

39. […] the Committee urges the State party to: (a) Ensure that all forms of surveillance and acts relating to the right to privacy, including online surveillance conducted for State security reasons, are regulated by appropriate laws that fully comply with the Covenant, specifically article 17;

Concluding Observations on the Fourth Periodic Report of Hong Kong, China, Human Rights Committee, UN Doc CCPR/C/CHN-HKG/CO/4 (22 July 2022)

39. The Committee is concerned that section 3 (1) (a) of the Interception of Communications and Surveillance (Amendment) Ordinance, article 43 (6) of the National Security Law and schedule 6 of the implementation rules, which facilitate arbitrary intrusion of privacy for the purposes of public security or national security, are not compatible with article 17 of the Covenant. […]

40. Hong Kong, China, should:
(a) Pending the repeal of the National Security Law, refrain from applying article 43 (6) thereof and schedule 6 of the implementation rules;
(b) Take concrete steps to bring the Interception of Communications and Surveillance (Amendment) Ordinance and the Personal Data (Privacy) (Amendment) Ordinance 2021 into line with article 17 of the Covenant;

Concluding Observations on the Fifth Periodic Report of Belarus, Human Rights Committee, UN Doc CCPR/C/BLR/CO/5 (22 November 2018)

43. The Committee is concerned at reports that legislation provides for broad powers of surveillance and that the interception of all electronic communications, including through the system of operative investigative measures, which allows remote access to all user communications without notifying providers, does not afford sufficient safeguards against arbitrary interference with the privacy of individuals (art. 17).

44. The State party should ensure that: (a) all types of surveillance activities and interference with

privacy, including online surveillance for the purposes of State security, are governed by appropriate legislation that is in full conformity with the Covenant, in particular article 17, including with the principles of legality, proportionality and necessity, and that State practice conforms thereto; […]

Concluding Observations on the Seventh Periodic Report of Norway, Human Rights Committee, UN Doc CCPR/C/NOR/CO/7 (25 April 2018)

21. The State party […] should ensure that the collection and use of data on communications take place on the basis of specific and legitimate objectives and that the exact circumstances in which such interference may be authorized and the categories of persons likely to be placed under surveillance are set out in detail in law. It should also ensure the effectiveness and independence of a monitoring system for surveillance activities."

Concluding Observations on the Fourth Periodic Report of Rwanda, Human Rights Committee, UN Doc CCPR/C/RWA/CO/4 (2 May 2016)

36. […] It should also ensure that communications are intercepted and data are used to achieve specific and legitimate objectives and that the categories of circumstances in which such interference may be authorized and the categories of persons whose communications are likely to be intercepted are set out in detail. [...]

Concluding Observations on the Fifth Periodic Report of France, Human Rights Committee, UN Doc CCPR/C/FRA/CO/5 (17 August 2015)

12. […] The State party should ensure that the collection and use of data on communications take place on the basis of specific and legitimate objectives and that the exact circumstances in which such interference may be authorized and the categories of persons likely to be placed under surveillance are set out in detail.

UN Human Rights Committee, General Comment No 16: Article 17 (Right to Privacy), UN Doc HRI/GEN/1/Rev.1 (8 April 1988)

10. The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. […]

***Antonius Cornelis Van Hulst v Netherlands*, Comm No 903/1999, Human Rights Committee, UN Doc CCPR/C/82/D903/1999 (15 November 2004)**

7.3 The Committee recalls that, in order to be permissible under article 17, any interference with the right to privacy must cumulatively meet several conditions set out in paragraph 1, i.e. it must be provided for by law, be in accordance with the provisions, aims and objectives of the Covenant and be reasonable in the particular circumstances of the case.

African Commission on Human and Peoples' Rights, Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa, ACHPR/Res.573 (LXXVII) (9 November 2023)

Recognizing the lack of adequate national frameworks on privacy, communication surveillance and the protection of personal data;

***Škoberne v Slovenia*, App No 19920/20, Judgment, European Court of Human Rights (15 February 2024)**

120. […] In cases where the legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question of whether the "necessity" test

has been complied with; it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements. The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society" – in particular by providing adequate and effective safeguards and guarantees against abuse (see *Roman Zakharov*, § 236; *Kennedy*, § 155; and *Big Brother Watch and Others*, § 334, all cited above).

123. With respect to the bulk interception of data relating to international communications, the Court has considered that the degree of interference with individuals' Article 8 rights increases as the process progresses (*Big Brother Watch and Others*, cited above, § 325). It has however observed that even the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (ibid., § 330). In that regard, the Court has found it imperative that when a State is operating a bulk-interception regime, domestic law should set out detailed rules regarding when the authorities might resort to such measures. In particular, domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorised. Moreover, as defined in previous case-law, the domestic law should set out a limit on the duration of interception, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted data may or must be erased or destroyed (ibid., § 348; see also *Centrum för rättvisa*, cited above, § 262). […]

***Podchasov v Russia*, App No 33696/19, Judgment, European Court of Human Rights (13 February 2024)**

54. It is true that there is no evidence that the authorities accessed the applicant's data stored by Telegram. Since it is impossible for an individual or a legal person to know for certain whether their data has been accessed, it is appropriate to analyse the question whether the applicant may claim that he is a victim of interference with his rights under Article 8 owing to the mere existence of laws permitting authorities to do so with reference to the same criteria as the ones used in relation to secret surveillance (see *Ekimdzhiev and Others*, cited above, § 376).

55. […] The mere existence of the contested legislation therefore amounts in itself to an interference with the exercise of the applicant's rights under Article 8 (compare *Ekimdzhiev and Others*, cited above, §§ 383-84).

61. […] The wording "in accordance with the law" requires the impugned measure to have some basis in domestic law. It must also be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must therefore be accessible to the person concerned and foreseeable as to its effects (see *Roman Zakharov,* cited above, §§ 227-28).

63. In the context of the collection and processing of personal data, it is essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness (ibid., § 99; see also *P.N. v. Germany*, no. 74440/17, § 62, 11 June 2020). The domestic law should notably ensure that retained data are relevant and not excessive in relation to the purposes for which they are stored, and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. The domestic law must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse (see *S. and Marper*, cited above, § 103). […]

***Plechlo v Slovakia*, App No 18593/19, Judgment, European Court of Human Rights (26 October 2023)**

43. As to the requirement for such interference to be "in accordance with the law" under Article 8 § 2, this expression in general requires, first, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be compatible with the rule of law and accessible to the person concerned, who must, moreover, be able to foresee its consequences for him or her. In that regard, it has been recognised that, where a power of the executive is exercised in secret, the risks of arbitrariness are evident. Thus, the domestic law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to any such measures. Furthermore, the Court has acknowledged that, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference. Furthermore, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist guarantees against abuse which are adequate and effective. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law (see, for example, *Dragojević*, cited above, §§ 80-83, with further references).

***Svetova and Others v Russia*, App No 54714/17, Judgment, European Court of Human Rights (24 January 2023)**

37. The Court considers, first, that the search of the applicants' flat and the seizure of the applicants' personal belongings constituted an interference with the exercise of the applicants' right to respect for their private life and home within the meaning of Article 8 § 1 of the Convention (see *Avaz Zeynalov v. Azerbaijan*, nos. 37816/12 and 25260/14, § 78, 22 April 2021, with further references). Such interference will constitute a breach of Article 8 unless it is "in accordance with the law", pursues one or more of the legitimate aims referred to in Article 8 § 2 and is "necessary in a democratic society" to achieve those aims.

***Potoczká and Adamčo v Slovakia*, App No 7286/16, Judgment, European Court of Human Rights (12 January 2023)**

71. As to the requirement for such interference to be "in accordance with the law" under Article 8 § 2, it in general requires, first, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be compatible with the rule of law and accessible to the person concerned, who must, moreover, be able to foresee its consequences for him or her. In that regard, it has been recognised that, where a power of the executive is exercised in secret, the risks of arbitrariness are evident. Thus, the domestic law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to any such measures. Furthermore, the Court has acknowledged that, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference. Furthermore, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist guarantees against abuse which are adequate and effective. This assessment depends on all the circumstances of the case, such as the

nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law (see, for example, *Dragojević*, cited above, §§ 80-83, with further references).

***Haščak v Slovakia*, Apps Nos 58359/12 and 2 others, Judgment, European Court of Human Rights (23 June 2022)**

89. As regards the compatibility of that interference with the requirements of the second paragraph of that Article, and in particular with the requirement for that interference to be "in accordance with the law", the Court would again refer to the general principles cited in cited in *Zoltán Varga* (§ 150 and 151). It reiterates especially that, where a power of the executive is exercised in secret, the risks of arbitrariness are evident. Since the implementation in practice of measures of secret surveillance is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference (see, for example, *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 76, ECHR 2006-VII, with further references).

94. Having considered all other means of legal protection against arbitrary interference (ibid., §§ 158-61), the Court concluded in *Zoltán Varga* that – in view of the lack of clarity of the applicable jurisdictional rules and the lack of procedures for the implementation of the existing rules and flaws in their application – when implementing the warrants the SIS had practically enjoyed discretion amounting to unfettered power, which had not been accompanied by a measure of protection against arbitrary interference, as required by the rule of law. It had accordingly not been "in accordance with the law" for the purposes of Article 8 § 2 of the Convention (ibid., § 162).

***Nuh Uzun and Others v Türkiye*, App No 49341/18 and 13 others, Judgment, European Court of Human Rights (29 March 2022) (translated from the original French)**

84. The Court reiterates its settled case-law to the effect that the words "laid down by law" mean that the measure at issue must have a basis in domestic law and be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention and is inherent in the object and purpose of Article 8. The law must therefore be sufficiently accessible and foreseeable, that is to say stated with sufficient precision to enable the individual - if necessary with the assistance of enlightened counsel - to regulate his [or her] conduct. If it is to be regarded as complying with these requirements, it must provide adequate protection against arbitrariness and, accordingly, define with sufficient clarity the scope and manner of exercise of the power conferred on the competent authorities (see *S. and Marper*, cited above, § 95, and *Rotaru*, cited above, § 55).

***Vasil Vasilev v Bulgaria*, App No 7610/15, Judgment, European Court of Human Rights (16 November 2021)**

88. The expression "in accordance with the law" in Article 8 § 2 of the Convention does not merely require compliance with domestic law; it additionally implies that that law be accessible, sufficiently foreseeable and compatible with the rule of law (see *Malone*, § 67; *Kopp*, § 55; and *Amann*, §§ 50 and 55, all cited above).

89. The covert interception and recording of a telephone conversation is a serious interference with the rights enshrined in Article 8 of the Convention and must hence be based on a "law" which is particularly precise; it is essential to have clear, detailed rules on the subject (see *Kopp*, cited above, § 72). […]

***Azer Ahmadov v Azerbaijan*, App No 3409/10, Judgment, European Court of Human Rights (22 July 2021)**

63. […] the wording "in accordance with the law" requires the impugned measure to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects (see, for example, *Kruslin v. France*, 24 April 1990, § 27, Series A no. 176-A, and *Kvasnica v. Slovakia*, no. 72094/01, § 78, 9 June 2009).

***Zoltán Varga v Slovakia*, App No 58361/12 and 2 others, Judgment, European Court of Human Rights (20 July 2021)**

151. As regards the criterion "in accordance with the law", the Court reiterates its settled case-law according to which this criterion not only requires the impugned measure to have some basis in domestic law, but also refers to the quality of the law in question, meaning that it should be accessible to the person concerned and foreseeable as to its effects. The law must be compatible with the rule of law, which means that it must provide a measure of legal protection against arbitrary interference by public authorities with the rights safeguarded by paragraph 1 of Article 8. Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident. Since the implementation in practice of measures of secret surveillance is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference […]."

***Berlizev v Ukraine*, App No 43571/12, Judgment, European Court of Human Rights (8 July 2021)**

39. The expression "in accordance with the law" in Article 8 § 2 of the Convention, in essence, refers back to national law and states the obligation to conform to the substantive and procedural rules thereof (see *Akopyan v. Ukraine*, no. 12317/06, § 109, 5 June 2014). Where it has been shown that the interference was not in accordance with the law, a violation of Article 8 of the Convention will normally be found without investigating whether the interference pursued a 'legitimate aim' or was 'necessary in a democratic society'" (see *Giorgi Nikolaishvili v. Georgia*, no. 37048/04, § 129, 13 January 2009).

***Big Brother Watch and 15 Others v The United Kingdom*, Apps Nos 58170/13, 62322/14 and 24960/15, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

332. Any interference with an individual's Article 8 rights can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which that paragraph refers and is necessary in a democratic society in order to achieve any such aim (see *Roman Zakharov*, cited above, § 227; see also *Kennedy v the United Kingdom*, no. 26839/05, § 130, 18 May 2010). The wording "in accordance with the law" requires the impugned measure to have some basis in domestic law (as opposed to a practice which does not have a specific legal basis – see *Heglas v the Czech Republic*, no. 5935/02, § 74, 1 March 2007). It must also be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must therefore be accessible to the person concerned and foreseeable as to its effects (see *Roman Zakharov*, cited above, § 228; see also, among many other authorities, *Rotaru*, cited above, § 52; *S. and Marper*, cited above, § 95, and *Kennedy*, cited above, § 151).

334. […] The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied

only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards and guarantees against abuse.

148. It is clear that the first two of the six "minimum safeguards" which the Court, in the context of targeted interception, has found should be defined clearly in domestic law in order to avoid abuses of power (that is, the nature of offences which may give rise to an interception order and the categories of people liable to have their communications intercepted: see paragraph 335 above), are not readily applicable to a bulk interception regime. Similarly, the requirement of "reasonable suspicion", which can be found in the Court's case-law on targeted interception in the context of criminal investigations is less germane in the bulk interception context, the purpose of which is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence. Nevertheless, the Court considers it imperative that when a State is operating such a regime, domestic law should contain detailed rules on when the authorities may resort to such measures. In particular, domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorised and the circumstances in which an individual's communications might be intercepted. The remaining four minimum safeguards defined by the Court in its previous judgments — that is, that domestic law should set out a limit on the duration of interception, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted data may or must be erased or destroyed — are equally relevant to bulk interception.

***Centrum för Rättvisa v Sweden*, App No 35252/08, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

262. It is clear that the first two of the six "minimum safeguards" which the Court, in the context of targeted interception, has found should be defined clearly in domestic law in order to avoid abuses of power (that is, the nature of offences which may give rise to an interception order and the categories of people liable to have their communications intercepted: see paragraph 249 above), are not readily applicable to a bulk interception regime. Similarly, the requirement of "reasonable suspicion", which can be found in the Court's case-law on targeted interception in the context of criminal investigations is less germane in the bulk interception context, the purpose of which is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence. Nevertheless, the Court considers it imperative that when a State is operating such a regime, domestic law should contain detailed rules on when the authorities may resort to such measures. In particular, domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorised and the circumstances in which an individual's communications might be intercepted. The remaining four minimum safeguards defined by the Court in its previous judgments — that is, that domestic law should set out a limit on the duration of interception, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted data may or must be erased or destroyed — are equally relevant to bulk interception."

***Gorlov and Others v Russia*, App No 27057/06, European Court of Human Rights, Judgment (2 July 2019)**

85. The Court further reiterates that the expression "in accordance with the law", within the meaning of Article 8 § 2 of the Convention, requires the impugned measure to have some basis in domestic law and be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise […]. The Court must thus also be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as

the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.

88. […] Whilst those legal provisions set forth a general rule enabling the administrations of penal institutions and pre-trial detention centres to have recourse to video surveillance, they provide no further details in that respect.

92. Furthermore, the document in question is classified as being "for internal use only", with the result that its contents are not accessible to the general public. At the same time, the applicants acknowledged that, upon their arrival at the relevant detention facilities, they had been made aware of the fact that would be placed under permanent video surveillance (see paragraph 63). Against this background, the Court finds it reasonable to assume that the contents of the document under examination, at least the relevant part, was made sufficiently accessible to the applicants.

96. In the present case, however, the applicants' placement under permanent video surveillance was not based on an individualised and reasoned decision providing reasons which would have justified the measure in question in the light of the legitimate aims pursued; the contested measure was not limited in time, and the administrations of the penal institutions or pre trial detention centre as the case may be were not under an obligation to review regularly (or at all) the well-foundedness of that measure. Indeed, there does not appear to exist any basis in national law for the adoption of such individualised decisions, the Supreme Court of Russia noting in its decision of 12 March 2014 that the existing legal framework "[did] not provide for the adoption of any [individualised] decision [authorising] the use of technical means of control and supervision" […].

97. In such circumstances, whilst the Court is prepared to accept that the contested measure had some basis in national law, it is not convinced that the existing legal framework is compatible with the "quality of law" requirement…[I]t does not define with sufficient clarity the scope of those powers and the manner of their exercise so as to afford an individual adequate protection against arbitrariness. […] As it stands, the national law offers virtually no safeguards against abuse by State officials.

***Ben Faiza v France*, App No 31446/12, Judgment, European Court of Human Rights (8 February 2018) (translated from the original French)**

58. [...] Article 81 of the CPP, applied in this case, merely refers to a concept of very general scope, namely "acts of information which it deems useful for the manifestation of the truth". Moreover, the Court recalls that it has already found, in connection with telephone tapping cases, that Article 81 of the CPP, even when read in combination with other provisions of the CPP, did not offer sufficient "foreseeability" as required by Article 8 of the Convention. The fact that surveillance of GPS movements allegedly constitutes a less intrusive interference with private life that the interception of telephone conversations, is not, in itself, likely to call into question this finding, and all the more it has added to other measures of observation. In addition, the Court notes that the vagueness of the French law at the time of the facts cannot be compensated by the jurisprudence of the domestic courts, […]

***Dudchenko v Russia*, App No 37717/05, Judgment, European Court of Human Rights (7 November 2017)**

91. The wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects.

***Konstantin Moskalev v Russia*, App No 59589/10, Judgment, European Court of Human Rights (7 November 2017)**

47. The wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects.

50. Although the applicant did not complain that the quality of the domestic law had fallen short of the Convention standards, when examining whether the interference complained of was "in accordance with the law", the Court must assess the quality of the relevant domestic law in relation to the requirements of the fundamental principle of the rule of law. The Court notes in this connection that in the case of *Roman Zakharov* (cited above) it has already found that Russian law does not meet the "quality of law" requirement because the legal provisions governing the interception of communications do not offer adequate and effective guarantees against arbitrariness and the risk of abuse. They are therefore incapable of keeping the "interference" to what is "necessary in a democratic society. […]

***Akhlyustin v Russia*, App No 21200/05, Judgment, European Court of Human Rights (7 November 2017)**

45. It follows that in the instant case, as in the *Bykov* case, the applicant enjoyed very few, if any, safeguards in the procedure by which the surveillance measures against him were ordered and implemented. In particular, the legal discretion of the authorities to order the "surveillance" was not subject to any conditions, and its scope and the manner in which it was exercised were not defined; no other specific safeguards were provided for. Given the absence of specific regulations providing safeguards, the Court is not satisfied that the possibility, provided for by Russian law, for the applicant to bring court proceedings seeking to declare the surveillance unlawful or to request the exclusion of its results as unlawfully obtained evidence met the "quality of law" requirements described above […]

46. The Court concludes that the covert surveillance measures against the applicant were not accompanied by adequate safeguards against various possible abuses. They were open to arbitrariness and were therefore inconsistent with the requirement of lawfulness. The interference with the applicant's right to respect for his private life was not "in accordance with the law", as required by Article 8 § 2 of the Convention. In the light of this conclusion, the Court is not required to determine whether the interference was "necessary in a democratic society" for one of the aims enumerated in paragraph 2 of Article 8.

***Roman Zakharov v Russia*, App No 47143/06, Judgment, European Court of Human Rights (4 December 2015)**

238. The Court will therefore assess in turn the accessibility of the domestic law, the scope and duration of the secret surveillance measures, the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data, the authorisation procedures, the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law.

***Uzun v Germany*, App No 35623/05, Judgment, European Court of Human Rights (2 September 2010)**

63. [...] in the context of secret measures of surveillance by public authorities, because of the lack of public scrutiny and the risk of misuse of power, compatibility with the rule of law requires that domestic law provides adequate protection against arbitrary interference with Article 8 rights. The

Court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law […]

***Bykov v Russia*, App No 4378/02, Judgment, Grand Chamber, European Court of Human Rights (10 March 2009)**

76. The Court reiterates that the phrase "in accordance with the law" not only requires compliance with domestic law but also relates to the quality of that law, requiring it to be compatible with the rule of law. In the context of covert surveillance by public authorities, in this instance the police, domestic law must provide protection against arbitrary interference with an individual's right under Article 8. Moreover, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures. […]

78. The Court has consistently held that when it comes to the interception of communications for the purpose of a police investigation, "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence". In particular, in order to comply with the requirement of the "quality of the law", a law which confers discretion must indicate the scope of that discretion, although the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law. The degree of precision required of the "law" in this connection will depend upon the particular subject-matter. Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive – or to a judge – to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.

79. In the Court's opinion, these principles apply equally to the use of a radio-transmitting device, which, in terms of the nature and degree of the intrusion involved, is virtually identical to telephone tapping.

80. In the instant case, the applicant enjoyed very few, if any, safeguards in the procedure by which the interception of his conversation with V. was ordered and implemented. In particular, the legal discretion of the authorities to order the interception was not subject to any conditions, and the scope and the manner of its exercise were not defined; no other specific safeguards were provided for. Given the absence of specific regulations providing safeguards, the Court is not satisfied that, as claimed by the Government, the possibility for the applicant to bring court proceedings seeking to declare the "operative experiment" unlawful and to request the exclusion of its results as unlawfully obtained evidence met the above requirements.

***Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, App No 62540/00, Judgment, European Court of Human Rights (28 June 2007)**

71. The expression "in accordance with the law", as used in Article 8 § 2, does not only require that the impugned measure should have some basis in domestic law. It also refers to the quality of this law, demanding that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him or her, and compatible with the rule of law.

***Weber and Saravia v Germany*, App No 54934/00, Decision, European Court of Human Rights (29 June 2006)**

84. The Court reiterates that the expression "in accordance with the law" within the meaning of Article 8 § 2 requires, firstly, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law. […]

***Taylor-Sabori v The United Kingdom*, App No 47114/99, Judgment, European Court of Human Rights (22 October 2002)**

18. […] It recalls that the phrase "in accordance with the law" not only requires compliance with domestic law but also relates to the quality of that law, requiring it to be compatible with the rule of law. In the context of covert surveillance by public authorities, in this instance the police, domestic law must provide protection against arbitrary interference with an individual's right under Article 8. Moreover, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures.

***Escher et al. v Brazil*, Inter-American Court of Human Rights, Judgment (on Preliminary Objections, Merits, Reparations, and Costs) Series C No 200 (6 July 2009)**

131. Taking into account that telephone interception can represent a serious interference in the private life of an individual, this measure must be based on a law that must be precise and indicate the corresponding clear and detailed rules, such as the circumstances in which this measure can be adopted, the persons authorized to request it, to order it and to carry it out, and the procedure to be followed.

***Ms X and Y v Argentina*, Inter-American Commission on Human Rights, Case 10.506, Report No 38/96 (15 October 1996)**

91. […] The object of Article 11, as well as of the entire Convention, is essentially to protect the individual against arbitrary interference by public officials. Nevertheless, it also requires the state to adopt all necessary legislation in order to ensure this provision's effectiveness. The right to privacy guarantees that each individual has a sphere into which no one can intrude, a zone of activity which is wholly one's own. In this sense, various guarantees throughout the Convention which protect the sanctity of the person create zones of privacy.

92. Article 11.2 specifically prohibits "arbitrary or abusive" interference with this right. This provision indicates that in addition to the condition of legality, which should always be observed when a restriction is imposed on the rights of the Convention, the state has a special obligation to prevent "arbitrary or abusive" interferences. The notion of "arbitrary interference" refers to elements of injustice, unpredictability and unreasonableness which were already considered by this Commission when it addressed the issues of the necessity, reasonableness, and proportionality of the searches and inspections.

***Spetsializirana prokuratura* (C-350/21), Judgment, Court of Justice of the European Union (17 November 2022) (translated from the original French)**

60. In the light of all the foregoing considerations, the answer to the first question referred for a preliminary ruling is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which provides, as a preventive measure, for the purposes of combating serious crime and preventing serious threats to public security, general and indiscriminate retention of traffic data and location data, even if that legislation limits such general and indiscriminate retention to a period of six months

and provides for a number of safeguards as regards retention of and access to the data in question. […]

65. It follows that national legislation relating to the storage of and access to personal data must contain provisions making it clear, in a clear and precise manner, that access to stored data must be limited to what is strictly necessary to achieve the objective pursued by that storage.

66. It is for the national court to ascertain whether the national legislation at issue in the main proceedings complies with that requirement, taking into account, in particular, the fact that that legislation appears to be limited, as regards the extent of the access to be granted, to requiring that it relate only to a reasonable period of time not exceeding six months.

***Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH* (C 793/19 and C 794/19), Judgment, Grand Chamber, Court of Justice of the European Union (20 September 2022)**

75. However, the Court specified that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not preclude legislative measures that, for the purposes of combating serous crime and preventing serious threats to public security, provide for:

- the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;
- the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;–the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and
- recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention (quick freeze) of traffic and location data in the possession of those service providers, provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse (judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168, and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 67).

A measure providing for general and indiscriminate retention of the majority of traffic and location data for a period of several weeks.

77. In the first place, as regards the extent of the data retained, it is apparent from the order for reference that, in the context of the provision of telephone services, the retention obligation laid down by that legislation covers, inter alia, the data necessary to identify the source of a communication and its destination, the date and time of the start and end of the communication or – in the case of communication by SMS, multimedia message or similar message – the time of dispatch and receipt of the message and, in the case of mobile use, the designation of the cell sites used by the caller and the recipient at the start of the communication. In the context of the provision of internet access services, the retention obligation covers, inter alia, the IP address assigned to the subscriber, the date and time of the start and end of internet use from the assigned IP address and, in the case of mobile use, the designation of the cell sites used at the beginning of the internet connection. The data enabling the identification of the geographical location and the directions of maximum radiation of the antennas serving the cell site in question are also retained.

78. Although the national legislation at issue in the main proceedings excludes the content of the communication and the data concerning the websites visited from the retention obligation and requires the retention of the cell site designation only at the beginning of the communication, that was also true, in essence, of the national legislation transposing Directive 2006/24 at issue in the cases that gave rise to the judgment of 6 October 2020, La Quadrature du Net and Others (C-511/18, C-512/18 and C-520/18, EU:C:2020:791). Despite those limitations, the Court held in that judgment that the categories of data retained under that directive and those national rules could allow very precise conclusions to be drawn concerning the private life of the persons concerned, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them and, in particular, provide the means of establishing a profile of those persons.

79. It must also be noted that, although the legislation at issue in the main proceedings does not cover the data concerning the websites visited, it nevertheless provides for the retention of IP addresses. Since IP addresses may be used, among other things, to track an internet user's complete clickstream and, therefore, his or her entire online activity, those data enable a detailed profile of the user to be established. Thus, the retention and analysis of those IP addresses which is required for such tracking constitute a serious interference with the fundamental rights of the internet user enshrined in Articles 7 and 8 of the Charter (see, to that effect, judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 153). […]

83. It is therefore apparent from the order for reference that the retention of traffic and location data provided for by that national legislation concerns practically the entire population without those persons being, even indirectly, in a situation liable to give rise to criminal prosecutions. Similarly, that legislation requires the general retention, without a reason, and without any distinction in terms of personal, temporal or geographical factors, of most traffic and location data, the scope of which corresponds, in essence, to that of the data retained in the cases which led to the case-law referred to in paragraph 78 above.

84. Accordingly, in the light of the case-law cited in paragraph 75 above, a data retention obligation such as that at issue in the main proceedings cannot be regarded as a targeted retention of data, contrary to the submissions of the German Government.

106. The Court stated, in that regard, that, while the objective evidence may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the persons thus targeted may, in particular, be persons who have been identified beforehand, in the course of the applicable national procedures and on the basis of objective and non-discriminatory factors, as posing a threat to public or national security in the Member State concerned (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 77).

***Ligue des droits humains v Conseil des ministres* (C-817/19), Judgment, Grand Chamber, Court of Justice of the European Union (21 June 2022)**

78. […] the Court has held that, in so far as Directive 2016/680 defines, in Article 3(7) thereof, the concept of 'competent authority', such a definition must be applied, by analogy, to Article 2(2)(d) of the GDPR (see, to that effect, judgment of 22 June 2021, Latvijas Republikas Saeima (Penalty points), C-439/19, EU:C:2021:504, paragraph 69).

79. Pursuant to Articles 4 and 7 of the PNR Directive, each Member State must, respectively, designate, as its PIU, an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime and adopt a list of the competent authorities entitled to request or receive PNR data or the result of processing those data from the PIU, the latter authorities being also competent for those purposes, as specified in Article 7(2) of that directive. […]

114. It should be added that the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the act which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned, bearing in mind, on the one hand, that that requirement does not preclude the limitation in question from being formulated in terms which are sufficiently open to be able to adapt to different scenarios and keep pace with changing circumstances (see, to that effect, judgment of 26 April 2022, Poland v Parliament and Council, C-401/19, EU:C:2022:297, paragraphs 64 and 74 and the case-law cited) and, on the other hand, that the Court may, where appropriate, specify, by means of interpretation, the actual scope of the limitation in the light of the very wording of the EU legislation in question as well as its general scheme and the objectives it pursues, as interpreted in view of the fundamental rights guaranteed by the Charter. […]

120. As regards respect for the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter, it is true that PNR data may, in some circumstances, reveal very specific information on the private life of a person. However, in so far as, on the one hand, the nature of that information is limited to certain aspects of a person's private life, concerning that person's air travel in particular, and, on the other hand, the PNR Directive expressly prohibits in Article 13(4) thereof the processing of sensitive data within the meaning of Article 9(1) of the GDPR, the data covered by that directive do not by themselves allow for a full overview of the private life of a person. In addition, that directive, in Article 1(2) thereof read in conjunction with Article 3(8) and (9) thereof as well as Annex II thereto, circumscribes the purposes for which those data are to be processed. Lastly, that same directive, in Articles 4 to 15 thereof, lays down the rules governing the transfer, processing and retention of those data as well as the rules intended to ensure, inter alia, the security, confidentiality and integrity of those data, and to protect them against unlawful access and processing. In those circumstances, the interferences which the PNR Directive entails do not adversely affect the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter. […]

262. In the light of the foregoing, the answer to the Question 8 is that Article 12(1) of the PNR Directive, read in conjunction with Articles 7 and 8 as well as Article 52(1) of the Charter, must be interpreted as precluding national legislation which provides for a general retention period of five years for PNR data, applicable indiscriminately to all air passengers, including those for whom neither the advance assessment under Article 6(2)(a) of that directive nor any verification carried out during the period of six months referred to in Article 12(2) of the said directive nor any other circumstance have revealed the existence of objective material capable of establishing a risk that relates to terrorist offences or serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.

***G.D. v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, and Attorney General*, (C-140/20), Judgment, Grand Chamber, Court of Justice of the European Union (5 April 2022)**

42. Furthermore, it is clear from the third sentence in Article 15(1) of Directive 2002/58 that measures taken by the Member States must comply with the general principles of EU law, which include the principle of proportionality, and ensure respect for the fundamental rights guaranteed by the Charter. In that regard, the Court has previously held that the obligation imposed on providers of electronic communications services by a Member State by way of national legislation to retain traffic data for the purpose of making them available, if necessary, to the competent national authorities raises issues relating to compatibility not only with Articles 7 and 8 of the Charter, relating to the protection of privacy and to the protection of personal data, respectively, but also with Article 11 of the Charter, relating to the freedom of expression (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 113 and the case-law cited). […]

55. Thus, national legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the data to be retained and the objective pursued. In particular, as regards combating serious crime, the data whose retention is provided for must be capable of contributing to the prevention, detection or prosecution of serious offences (see, to that effect, judgments of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 59, and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 133). […]

66. In addition, the Court has emphasised that national legislation providing for the general and indiscriminate retention of traffic and location data covers the electronic communications of practically the entire population without any differentiation, limitation or exception being made in the light of the objective pursued. Such legislation is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with that objective of combating serious crime and, in particular, without there being any relationship between the data whose retention is provided for and a threat to public security. In particular, as the Court has already held, such legislation is not restricted to retention in relation to (i) data pertaining to a time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to combating serious crime (judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 143 and 144 and the case-law cited).

67. However, in paragraph 168 of the judgment of 6 October 2020, La Quadrature du Net and Others (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), the Court stated that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, does not preclude legislative measures that provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for

- the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;
- the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;
- the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and
- recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention (quick freeze) of traffic and location data in the possession of those service providers,

provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse. […]

77. The Court stated, in that regard, that, while the objective evidence may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the persons thus targeted may, in particular, be persons who have been identified beforehand, in the course of the applicable national procedures and on the basis of objective and non-discriminatory factors, as posing a threat to public or national security in the Member State concerned (see, to that effect, judgments of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 110, and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 149). […]

97. It should be observed, first of all, that the fact of authorising access for the purpose of combating serious crime to traffic and location data which have been retained in a general and indiscriminate way would make that access depend upon facts that fall outside that objective, according to whether or not, in the Member State concerned there was a serious threat to national security as referred to in the preceding paragraph, whereas, in view of the sole objective of the fight against serious crime which must justify the retention of those data and access thereto, there is nothing to justify a difference in treatment, in particular, as between the Member States.

98. As the Court has already held, access to traffic and location data retained by providers in accordance with a measure taken under Article 15(1) of Directive 2002/58, which must be given effect in full compliance with the conditions resulting from the case-law interpreting Directive 2002/58, may, in principle, be justified only by the public interest objective for which those providers were ordered to retain those data. It is otherwise only if the importance of the objective pursued by access is greater than that of the objective which justified retention (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 165 and 166).

99. The Danish Government's submission refers to a situation in which the objective pursued by the access request proposed, namely the fight against serious crime, is of lesser importance in the hierarchy of objectives of public interest than that which justified the retention, namely the safeguarding of national security. To authorise, in that situation, access to retained data would be contrary to that hierarchy of public interest objectives recalled in the preceding paragraph, and also to paragraphs 53, 56, 57 and 59 of this judgment.

100. In addition and moreover, in accordance with the case-law recalled in paragraph 65 of this judgment, traffic and location data cannot be the object of general and indiscriminate retention for the purpose of combating serious crime and, therefore, access to those data cannot be justified for that same purpose. Where those data have exceptionally been retained in a general and indiscriminate way for the purpose of the safeguarding of national security against a genuine and present or foreseeable threat, in the circumstances referred to in paragraph 58 of this judgment, the national authorities competent to undertake criminal investigations cannot access those data in the context of criminal proceedings, without depriving of any effectiveness the prohibition on such retention for the purpose of combating serious crime, recalled in paragraph 65.

101. In the light of all of the foregoing considerations, the answer to the first, second and fourth questions is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding legislative measures which provide, as a preventive measure, for the purposes of combating serious crime and for the prevention of serious threats to public security, for the general and indiscriminate retention of traffic and location data. However, Article 15(1), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not preclude legislative measures that, for the purposes of combating serious crime and preventing serious threats to public security, provide for:

- the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;
- the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;
- the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and
- recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,

provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.

102. By its third question, the referring court asks, in essence, whether, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation pursuant to which the centralised processing of requests for access to retained data, issued by the police in the context of the investigation or prosecution of serious criminal offences, is the responsibility of a police officer, assisted by a unit established within the police service which enjoys a degree of autonomy in the exercise of its duties and whose decisions may subsequently by subject to judicial review.

103. As a preliminary matter, it should be borne in mind that, while it is for national law to determine the conditions under which providers of electronic communications services must grant the competent national authorities access to data in their possession, the national legislation must, in order to satisfy the requirement of proportionality, as recalled in paragraph 54 of this judgment, lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that those data will be effectively protected against the risk of abuse (see, to that effect, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 48 and the case-law cited).

104. In particular, national legislation governing the access by the competent authorities to retained traffic and location data, adopted pursuant to Article 15(1) of Directive 2002/58, cannot be limited to requiring that the authorities' access to the data be consistent with the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use (judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications),* C-746/18, EU:C:2021:152, paragraph 49 and the case-law cited).

La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées; Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministers **(C-511/18, C-512/18 and C-520/18), Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2020)**

99. Article 4(2) TEU, to which the governments listed in paragraph 89 of the present judgment have made reference, cannot invalidate that conclusion. Indeed, according to the Court's settled case-law, although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law […].

104. It follows from the foregoing considerations that national legislation which requires providers of electronic communications services to retain traffic and location data for the purposes of protecting national security and combating crime, such as the legislation at issue in the main proceedings, falls within the scope of Directive 2002/58.

115. It should be made clear, in that regard, that the retention of traffic and location data constitutes, in itself, on the one hand, a derogation from the prohibition laid down in Article 5(1) of Directive 2002/58 barring any person other than the users from storing that data, and, on the other, an interference with the fundamental rights to respect for private life and the protection of personal data, enshrined in Articles 7 and 8 of the Charter, irrespective of whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference […].

116. Whether or not the retained data has been used subsequently is also irrelevant […], since access to such data is a separate interference with the fundamental rights referred to in the preceding paragraph, irrespective of the subsequent use made of it […].

121. Indeed, as can be seen from Article 52(1) of the Charter, that provision allows limitations to be placed on the exercise of those rights, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

***Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service* (C-623/17) Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2020)**

46. […] all operations processing personal data carried out by providers of electronic communications services fall within the scope of that directive, including processing operations resulting from obligations imposed on those providers by the public authorities, whereas those processing operations could, where appropriate, on the contrary, fall within the scope of the exception laid down in the first indent of Article 3(2) of Directive 95/46, given the broader wording of that provision, which covers all processing operations concerning public security, defence, or State security, regardless of the person carrying out those operations.

64. […] as can be seen from Article 52(1) of the Charter, that provision allows limitations to be placed on the exercise of those rights, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

65. It should be added that the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned […].

***Digital Rights Ireland Ltd v Minister of Communications, Marine and Natural Resources et al.* (C-293/12); *Kärntner Landesregierung and others* (C-594/12), Joined Cases, Judgment, Grand Chamber, Court of Justice of the European Union (8 April 2014)**

38. Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

I. ACCESSIBILITY REQUIREMENT

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

29. [S]ecret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of "law". Neither do laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion. The secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn,

demands greater precision in the rule governing the exercise of discretion, and additional oversight. Several States also require that the legal framework be established through primary legislation debated in parliament rather than simply subsidiary regulations enacted by the executive – a requirement that helps to ensure that the legal framework is not only accessible to the public concerned after its adoption, but also during its development, in accordance with article 25 of the International Covenant on Civil and Political Rights.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

50. As a primary step, Governments deploying surveillance tools must ensure that they do so in accordance with a domestic legal framework that meets the standards required by international human rights law […] To be compliant with those standards, national laws must: (b) Require that any legislation governing surveillance be contained in precise and publicly accessible laws.

***Malone v The United Kingdom*, App No 8691/79, Judgment, European Court of Human Rights (2 August 1984)**

70. The issue to be determined is therefore whether, under domestic law, the essential elements of the power to intercept communications were laid down with reasonable precision in accessible legal rules that sufficiently indicated the scope and manner of exercise of the discretion conferred on the relevant authorities. […]

79. [...] in its present state the law in England and Wales governing interception of communications for police purposes is somewhat obscure and open to differing interpretations […] on the evidence before the Court, it cannot be said with any reasonable certainty what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive. In view of the attendant obscurity and uncertainty as to the state of the law in this essential respect, the Court cannot but reach a similar conclusion to that of the Commission. In the opinion of the Court, the law of England and Wales does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities. To that extent, the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014)

36. Accessibility requires not only that domestic law be published, but also that it meet a standard of clarity and precision sufficient to enable those affected to regulate their conduct with foresight of the circumstances in which intrusive surveillance may occur… Prior to the introduction of mass surveillance programmes outlined in the present report, [it had always been understood that it was required for] domestic legislation to spell out clearly the conditions under which, and the procedures by which, any interference may be authorized; the categories of person whose communications may be intercepted; the limits on the duration of surveillance; and the procedures for the use and storage of the data collected. […]

60. […] there is an urgent need for States using [mass surveillance] technology to revise and update national legislation to ensure consistency with international human rights law. Not only is this a requirement of Article 17, but it also provides an important opportunity for informed debate that can raised public awareness and enable individuals to make informed choices. Where the privacy rights of the entire digital community are at stake, nothing short of detailed and explicit primary legislation should suffice.

***Haščak v Slovakia*, Apps Nos 58359/12 and 2 others, Judgment, European Court of Human Rights (23 June 2022)**

96. As to the storing of the derivative material from the implementation of the two warrants, under section 17(6) of the SIS Act, the Court found in *Zoltán Varga* that it had been subject to confidential rules which had been both adopted and applied by the SIS, with no element of external control. Such rules had clearly been lacking in accessibility and had provided Mr Varga with no protection against arbitrary interference with his right to respect for his private life (ibid., § 169). The retention of the said material had therefore not been "in accordance with the law" within the meaning of the second paragraph of Article 8 of the Convention (§ 171). These findings directly apply in the present case.

***Roman Zakharov v Russia*, App No 47143/06, Judgment, European Court of Human Rights (4 December 2015)**

239. It is common ground between the parties that almost all legal provisions governing secret surveillance… have been officially published and are accessible to the public. The parties disputed, however, whether the addendums to Order no 70 by the Ministry of Communications met the requirements of accessibility.

242. The publication of the Order in the Ministry of Communications' official magazine SvyazInform, distributed through subscription, made it available only to communications specialists rather than to the public at large. At the same time, the Court notes that the text of the Order, with the addendums, can be accessed through a privately-maintained internet legal database, which reproduced it from the publication in SvyazInform. The Court finds the lack of a generally accessible official publication of Order no 70 regrettable. However, taking into account the fact that it has been published in an official ministerial magazine, combined with the fact that it can be accessed by the general public through an internet legal database, the Court does not find it necessary to pursue further the issue of the accessibility of domestic law.

***Shimovolos v Russia*, App No 30194/09, Judgment, European Court of Human Rights (21 June 2011)**

69. Turning to the present case, the Court observes that the creation and maintenance of the Surveillance Database and the procedure for its operation are governed by ministerial order no 47. That order is not published and is not accessible to the public. The grounds for registration of a person's name in the database, the authorities competent to order such registration, the duration of the measure, the precise nature of the data collected, the procedures for storing and using the collected data and the existing controls and guarantees against abuse are thus not open to public scrutiny and knowledge.

70. For the above reasons, the Court does not consider that the domestic law indicates with sufficient clarity the scope and manner of exercise of the discretion conferred on the domestic authorities to collect and store in the Surveillance Database information on persons' private lives. In particular, it does not, as required by the Court's case-law, set out in a form accessible to the public any indication of the minimum safeguards against abuse. The interference with the applicant's rights under Article 8 was not, therefore, "in accordance with the law".

***Liberty and Others v The United Kingdom*, App No 58243/00, Judgment, European Court of Human Rights (1 July 2008)**

66. Under section 6 of the 1985 Act, the Secretary of State, when issuing a warrant for the interception of external communications, was called upon to "make such arrangements as he consider[ed] necessary" to ensure that material not covered by the certificate was not examined and that material that was certified as requiring examination was disclosed and reproduced only to the extent necessary. The applicants contend that material was selected for examination by an

electronic search engine, and that search terms, falling within the broad categories covered by the certificates, were selected and operated by officials. According to the Government, there were at the relevant time internal regulations, manuals and instructions applying to the processes of selection for examination, dissemination and storage of intercepted material, which provided a safeguard against abuse of power. The Court observes, however, that "arrangements" made under section 6 were not contained in legislation or otherwise made available to the public.

67. The fact that the Commissioner in his annual reports concluded that the Secretary of State's "arrangements" had been complied with, while an important safeguard against abuse of power, did not contribute towards the accessibility and clarity of the scheme, since he was not able to reveal what the "arrangements" were. In this connection the Court recalls its above case-law to the effect that the procedures to be followed for examining, using and storing intercepted material, inter alia, should be set out in a form which is open to public scrutiny and knowledge.

68. The Court notes the Government's concern that the publication of information regarding the arrangements made by the Secretary of State for the examination, use, storage, communication and destruction of intercepted material during the period in question might have damaged the efficacy of the intelligence-gathering system or given rise to a security risk. However, it observes that the German authorities considered it safe to include in the G10 Act, as examined in Weber and Saravia, express provisions about the treatment of material derived from strategic interception as applied to non-German telephone connections. In particular, the G10 Act stated that the Federal Intelligence Service was authorised to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order and which search terms had to be listed in the monitoring order. Moreover, the rules on storing and destroying data obtained through strategic monitoring were set out in detail in section 3(6) and (7) and section 7(4) of the amended G10 Act. The authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them. If that was not the case, they had to be destroyed and deleted from the files or, at the very least, access to them had to be blocked; the destruction had to be recorded in minutes and, in the cases envisaged in section 3(6) and section 7(4), had to be supervised by a staff member qualified to hold judicial office. The G10 Act further set out detailed provisions governing the transmission, retention and use of data obtained through the interception of external communications. In the United Kingdom, extensive extracts from the Code of Practice issued under section 71 of the 2000 Act are now in the public domain, which suggests that it is possible for a State to make public certain details about the operation of a scheme of external surveillance without compromising national security.

69. In conclusion, the Court does not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. The interference with the applicants' rights under Article 8 was not, therefore, "in accordance with the law".

II. FORESEEABILITY REQUIREMENT

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/7, 17 August 2015)

24. The State party should: […] (b) Ensure that any interference with the right to privacy with the family, with the home or with correspondence is authorized by laws that (i) are publicly

accessible; (ii) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (iii) are sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance, and procedures for the use and storage of data collected; and (iv) provide for effective safeguard against abuse.

***Podchasov v Russia*, App No 33696/19, Judgment, European Court of Human Rights (13 February 2024)**

64. In the context of secret surveillance, where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. To meet the requirement of "foreseeability", the domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see *Roman Zakharov,* cited above, §§ 229-30). […]

***Big Brother Watch and Others v The United Kingdom*, Apps Nos 58170/13, 62322/14 and 24960/15, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

333. The meaning of "foreseeability" in the context of secret surveillance is not the same as in many other fields. In the special context of secret measures of surveillance, such as the interception of communications, "foreseeability" cannot mean that individuals should be able to foresee when the authorities are likely to resort to such measures so that they can adapt their conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures. Moreover, the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference […].

423. […] However, these retention periods were only disclosed in the proceedings before this Court. Consequently, the shorter retention periods were not evident to anyone reading the IC Code; nor was there any indication in the IC Code that the retention periods for related communications data were different from those in respect of content. In the Court's view, in order to meet the Article 8 requirement of "foreseeability", the retention periods disclosed in the proceedings before it should be included in appropriate legislative and/or other general measures.

***Centrum för Rättvisa v Sweden*, App No 35252/08, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

247. […] In the special context of secret measures of surveillance, such as the interception of communications, "foreseeability" cannot mean that individuals should be able to foresee when the authorities are likely to resort to such measures so that they can adapt their conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on

secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures […]. Moreover, the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference […].

***Ivashchenko v Russia*, App No 61064/10, Judgment, European Court of Human Rights (13 February 2018)**

72. In addition, the phrase "in accordance with the law" (as well as "prescribed by law" in Article 10) requires the impugned measure to be compatible with the rule of law, which is mentioned in the preamble to the Convention and inherent in the object and purpose of Article 8 of the Convention. The "law" must thus be accessible to the person concerned and foreseeable as to its effects, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct.

73. For domestic law to meet these requirements it must afford a measure of legal protection against arbitrary interferences by public authorities with the rights safeguarded by the Convention. In matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate with sufficient clarity the scope of any such discretion conferred on the competent authorities and the manner of its exercise. The level of precision required of domestic legislation – which cannot in any case provide for every eventuality – depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed.

***Weber and Saravia v Germany*, App No 54934/00, Decision, European Court of Human Rights (29 June 2006)**

93. As to the third requirement, the law's foreseeability, the Court reiterates that foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures.

94. Moreover, since the implementation in practice of measures of secret surveillance of communication is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred to the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, UN Doc A/HRC/23/40 (17 April 2013)

83. Legal frameworks must ensure that communications surveillances measures: (a) are prescribed

by law, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application.

Concluding Observations on the Sixth Periodic Report of New Zealand, Human Rights Committee, UN Doc CCPR/C/NZL/CO/6 (28 April 2016)

15. The Committee is concerned that the right to privacy is not part of the Bill of Rights Act 1990 and that the existing legal framework provides the Government Communications Security Bureau with a very broad mandate. The Committee is also concerned about the absence of a clear definition of the terms "national security" and "private communication" in the Telecommunications (Interception Capability and Security) Act 2013. [...];

Concluding Observations on the Second Periodic Report of Namibia, Human Rights Committee, UN Doc CCPR/C/NAM/CO/2 (22 April 2016)

37. The Committee notes with concern that interception centres seem operational despite the fact that their legal basis, part 6 of the Communications Act, is not yet in force. While noting the indication by the delegation that all interceptions must be authorized by a magistrate, and that no private information is kept, the Committee is concerned about the lack of clarity regarding the reach of legal interception possibilities, as well as about the safeguards to ensure respect of the right to privacy in line with the Covenant.

Concluding Observations on the Fifth Periodic Report of Sri Lanka, Human Rights Committee, UN Doc CCPR/C/LKA/CO/5 (21 November 2014)

The State Party should [...] adopt national legislation that clearly and narrowly defines the exceptional conditions under which former combatants could be subject to monitoring and surveillance.

***Nuh Uzun and Others v Türkiye*, App No 49341/18 and 13 others, Judgment, European Court of Human Rights (29 March 2022) (translated from the original French)**

85. The degree of precision required of domestic legislation - which cannot, moreover, cover every eventuality - depends to a large extent on the content of the text in question, the area it is intended to cover and the number and quality of its addressees (see *Hassan and Tchaouch v. Bulgaria* [GC], no. 30985/96, § 84, ECHR 2000-XI, and the case-law cited therein).

86. With regard to personal data in particular, it is essential to lay down clear and detailed rules governing the scope and application of the measures and imposing minimum requirements designed to preserve the integrity and confidentiality of the data and the procedures for destroying them, so as to ensure that litigants have adequate safeguards (see *S. and Marper*, cited above, § 99, and the case-law references cited therein).

97. It should therefore be noted that the writings of 10 October 2016 and 1 March 2017 thus consisted of unpublished internal documents containing instructions from the Ministry of Justice addressed to the prisons. It must be observed that in those circumstances the documents were in principle not binding on those concerned (see, mutatis mutandis, *Amuur v. France*, 25 June 1996, § 53 [1996] ECR 996-III, and *Poltoratskiy v. Ukraine*, no. 38812/97, §§ 158-162, ECHR 2003-V), since their text had not been communicated to prisoners and convicts in any way (see, mutatis mutandis, *Silver and Others v. the United Kingdom*, 25 March 1983, § 93, Series A no. 61). A text of this nature, enacted outside the exercise of a normative power, cannot be regarded as a "law" of sufficient "quality" within the meaning of the Court's case-law, in that it could not offer adequate protection and the legal certainty necessary to prevent arbitrary infringements by the public authorities of the rights guaranteed by the Convention (see *Amuur*, cited above, § 53, and *Frérot v. France*, no. 70204/01, § 59, 12 June 2007).

98. Consequently, the Court considers that in the present case the interference at issue cannot be regarded as having been "prescribed by law" within the meaning of paragraph 2 of Article 8 of the Convention. In view of that conclusion, it considers that there is no need to ascertain whether the other conditions required by paragraph 2 of Article 8 of the Convention - namely the existence of a legitimate aim and the necessity of the interference in a democratic society - have been met in the present case.

***Ekimdzhiev and Ors v Bulgaria*, App No 70078/12, Judgment, European Court of Human Rights (11 January 2022)**

298. The relevant issue in relation to the grounds on which secret surveillance may be resorted to and the persons who can be placed under surveillance is whether the law authorising or permitting surveillance lays down with sufficient clarity (a) the nature of the offences and other grounds which may give rise to surveillance and (b) the categories of persons who may be placed under surveillance.

299. In Bulgaria, the law sets outs in an exhaustive manner the serious intentional criminal offences which can trigger the use of special means of surveillance (see paragraph 18 above). Moreover, it specifies that such means can be used only if there are grounds to suspect that such an offence is being planned, or is being or has been committed, and only if other methods of detection or investigation would be unlikely to succeed (see paragraphs 18 and 20 above). The law is thus sufficiently clear on that point (see *Roman Zakharov*, cited above, § 244). Indeed, it is clearer than when the Court first examined it and found it adequate in this respect in *Association for European Integration and Human Rights and Ekimdzhiev* (cited above, §§ 10 and 79). […]

302. The law also sets out in an exhaustive manner the categories of persons who, or objects which, may be placed under surveillance. When it comes to surveillance relating to criminal offences, the relevant categories are clearly defined: those are either people suspected of committing offences, people unwittingly used for their preparation or commission, people who have agreed to surveillance for their own protection, or cooperating witnesses in cases relating to a limited class of serious intentional offences, as well as objects capable of leading to the identification of such persons if their identity is unknown (see paragraph 23(a), (c), (d) and (e) above). It is true that when it comes to surveillance on national-security grounds, the law is couched in vaguer terms: "persons or objects related to national security" (see paragraph 23 (b) above). But the considerations in paragraph 301 above about the possibility of checking potential abuses flowing from the vagueness of the notion of national security are equally relevant here.

303. A problem arises, however, with the lack of sufficient precision about the meaning of the term "objects" in section 12(1) of the 1997 Act (see paragraph 23 (b) and (c) above). The Act does not clarify whether the "objects" which may be placed under surveillance – either because they relate to national security or because they are necessary to identify persons who need to be placed under surveillance – need to be concrete (for instance, specific premises, a specific vehicle, or a specific telephone line). It must be noted in this connection that the secret surveillance regime in Bulgaria is intended to be a targeted regime rather than a bulk one (compare with *Roman Zakharov*, cited above, § 265). Although an extreme example, the case of *Mustafa Sezgin Tanrıkulu* (cited above, §§ 51-60) illustrates the risk of misinterpretation of insufficiently precise legal provisions normally meant to permit only targeted surveillance to in reality enable large-scale surveillance. […] it tends to suggest that the Bulgarian courts are not averse to construing the term "objects" in section 12(1) of the 1997 Act in a rather extensive way.

***Benedik v Slovenia*, App No 62357/14, Judgment, European Court of Human Rights (24 April 2018)**

125. […], the Court reiterates that a rule is "foreseeable" if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct. In addition,

compatibility with the rule of law requires that domestic law provides adequate protection against arbitrary interference with Article 8 rights. The Court must thus be satisfied also that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.

***Szabó and Vissy v Hungary*, App No 37138/14, Judgment, European Court of Human Rights (12 January 2016)**

64. […] the wording of many statutes is not absolutely precise, and that the need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are vague. It is satisfied that even in the field of secret surveillance, where foreseeability is of particular concern, the danger of terrorist acts and the needs of rescue operations are both notions sufficiently clear so as to meet the requirements of lawfulness. For the Court, the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all situations that may prompt a decision to launch secret surveillance operations. The reference to terrorist threats or rescue operations can be seen in principle as giving citizens the requisite indication. For the Court, nothing indicates in the text of the relevant legislation that the notion of "terrorist acts", as used in section 7/E (1) a) (ad) of the Police Act, does not correspond to the crime of the same denomination contained in the Criminal Code.

65. However, in matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a discretion granted to the executive in the sphere of national security to be expressed in terms of unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.

66. The Court notes that under "section 7/E (3) surveillance", it is possible for virtually any person in Hungary to be subjected to secret surveillance. The legislation does not describe the categories of persons who, in practice, may have their communications intercepted. In this respect, the Court observes that there is an overlap between the condition that the categories of persons be set out and the condition that the nature of the underlying situations be clearly defined. The relevant circumstances which can give rise to interception, discussed in the preceding paragraphs, give guidance as to the categories of persons who are likely, in practice, to have their communications intercepted. Under the relevant Hungarian law, the proposal submitted to the responsible government minister must specify, either by name or as a range of persons, the person or persons as the interception subjects and/or any other relevant information capable of identifying them as well as the premises in respect of which the permission is sought.

67. It is of serious concern, however, that the notion of "persons concerned identified […] as a range of persons" might include indeed any person and be interpreted as paving the way for the unlimited surveillance of a large number of citizens. The Court notes the absence of any clarification in domestic legislation as to how this notion is to be applied in practice. For the Court, the category is overly broad, because there is no requirement of any kind for the authorities to demonstrate the actual or presumed relation between the persons or range of persons "concerned" and the prevention of any terrorist threat – let alone in a manner enabling an analysis by the authoriser which would go to the question of strict necessity with regard to the aims pursued and the means employed – although such an analysis appears to be warranted by section 53 (2) of the National Security Act, according to which "secret intelligence gathering [may only be applied] if the intelligence needed […] cannot be obtained in any other way".

***Roman Zakharov v Russia*, App No 47143/06, Judgment, European Court of Human Rights (4**

December 2015)

243. The Court reiterates that the national law must define the scope of application of secret surveillance measures by giving citizens an adequate indication as to the circumstances in which public authorities are empowered to resort to such measures – in particular by clearly setting out the nature of the offences which may give rise to an interception order and a definition of the categories of people liable to have their telephones tapped.

244. As regards the nature of the offences, the Court emphasises that the condition of foreseeability does not require States to set out exhaustively, by name, the specific offences which may give rise to interception. However, sufficient detail should be provided on the nature of the offences in question. Both the OSAA and the CCrP provide that telephone and other communications may be intercepted in connection with an offence of medium severity, a serious offence or an especially serious criminal offence – that is, an offence for which the Criminal Code prescribes a maximum penalty of more than three years' imprisonment – which has been already committed, is ongoing or being plotted. The Court considers that the nature of the offences which may give rise to an interception order is sufficiently clear. At the same time it notes with concern that Russian law allows secret interception of communications in respect of a very wide range of criminal offences, including for example, as pointed out by the applicant, pickpocketing.

245. The Court further notes that interceptions may be ordered not only in respect of a suspect or an accused, but also in respect of a person who may have information about an offence or may have other information relevant to the 12 […].

246. The Court also observes that in addition to interceptions for the purposes of preventing or detecting criminal offences, the OSAA also provides that telephone or other communications may be intercepted. following the receipt of information about events or activities endangering Russia's national, military, economic or ecological security. Which events or activities may be considered as endangering such types of security interests is nowhere defined in Russian law.

247. The Court has previously found that the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to subject an individual to secret surveillance on "national security" grounds. By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance. At the same time, the Court has also emphasised that in matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a discretion granted to the executive in the sphere of national security to be expressed in terms of unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.

248. It is significant that the OSAA does not give any indication of the circumstances under which an individual's communications may be intercepted on account of events or activities endangering Russia's national, military, economic or ecological security. It leaves the authorities an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse.

***Shimovolos v Russia*, App No 30194/09, Judgment, European Court of Human Rights (21 June 2011)**

68. The Court reiterates in this connection that in the special context of secret measures of surveillance the above requirements cannot mean that an individual should be able to foresee when the authorities are likely to resort to secret surveillance so that he can adapt his conduct accordingly.

However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on the application of secret measures of surveillance, especially as the technology available for use is continually becoming more sophisticated. The law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any measures of secret surveillance and collection of data. In addition, because of the lack of public scrutiny and the risk of abuse intrinsic to any system of secret surveillance, the following minimum safeguards should be set out in statute law to avoid abuses: the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.

***Uzun v Germany*, App No 35623/05, Judgment, European Court of Human Rights (2 September 2010)**

61. As to the requirement of legal "foreseeability" in this field, the Court reiterates that in the context of covert measures of surveillance, the law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any such measures. […]

62. The Court has further stated, in the context of Article 7 of the Convention, that in any system of law, including criminal law, however clearly drafted a legal provision may be, there is an inevitable element of judicial interpretation. There will always be a need for elucidation of doubtful points and for adaptation to changing circumstances. Indeed, in the Convention States, the progressive development of the criminal law through judicial law-making is a well entrenched and necessary part of legal tradition. The Convention cannot be read as outlawing the gradual clarification of the rules of criminal liability through judicial interpretation from case to case, provided that the resultant development is consistent with the essence of the offence and could reasonably be foreseen. The Court considers that these principles, developed under Article 7, apply also in the present context. […]

65. As to the law's foreseeability and its compliance with the rule of law, the Court notes at the outset that in his submissions, the applicant strongly relied on the minimum safeguards which are to be set out in statute law in order to avoid abuses as developed by the Court in the context of applications concerning the interception of telecommunications. According to these principles, the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their communications monitored; a limit on the duration of such monitoring; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which data obtained may or must be erased or the records destroyed, have to be defined in statute law.

***Kennedy v The United Kingdom*, App No 26839/05, Judgment, European Court of Human Rights (18 May 2010)**

159. As to the nature of the offences, the Court emphasises that the condition of foreseeability does not require States to set out exhaustively by name the specific offences which may give rise to interception. However, sufficient detail should be provided of the nature of the offences in question. In the case of RIPA, section 5 provides that interception can only take place where the Secretary of State believes that it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime or for the purposes of safeguarding the economic well-being of the United Kingdom. The applicant criticises the terms "national security" and "serious crime" as being insufficiently clear. The Court disagrees. It observes that the term "national security" is frequently employed in both national and international legislation and constitutes one of the legitimate aims to which Article 8 § 2 itself refers. The Court has previously emphasised that the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to deport an individual on "national security" grounds.

By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance. Similar considerations apply to the use of the term in the context of secret surveillance. Further, additional clarification of how the term is to be applied in practice in the United Kingdom has been provided by the Commissioner, who has indicated that it allows surveillance of activities which threaten the safety or well-being of the State and activities which are intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means. As for "serious crime", this is defined in the interpretative provisions of the Act itself and what is meant by "detecting" serious crime is also explained in the Act. The Court is of the view that the reference to serious crime, together with the interpretative clarifications in the Act, gives citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to secret surveillance measures. The Court therefore considers that, having regard to the provisions of RIPA, the nature of the offences which may give rise to an interception order is sufficiently clear.

160. The Court observes that under RIPA, it is possible for the communications of any person in the United Kingdom to be intercepted. However, it should be recalled that, in contrast to the *Liberty and Others* case which concerned the legislation on interception of communications between the United Kingdom and any other country, the present case concerns internal communications, i.e. communications within the United Kingdom. Further, the legislation must describe the categories of persons who, in practice, may have their communications intercepted. In this respect, the Court observes that there is an overlap between the condition that the categories of persons be set out and the condition that the nature of the offences be clearly defined. The relevant circumstances which can give rise to interception, discussed in the preceding paragraph, give guidance as to the categories of persons who are likely, in practice, to have their communications intercepted. Finally, the Court notes that in internal communications cases, the warrant itself must clearly specify, either by name or by description, one person as the interception subject or a single set of premises as the premises in respect of which the warrant is ordered. Names, addresses, telephone numbers and other relevant information must be specified in the schedule to the warrant. Indiscriminate capturing of vast amounts of communications is not permitted under the internal communications provisions of RIPA. The Court considers that, in the circumstances, no further clarification in the legislation or the Code of the categories of persons liable to have their communications intercepted can reasonably be required.

161. In respect of the duration of any telephone tapping, the Act clearly stipulates, first, the period after which an interception warrant will expire and, second, the conditions under which a warrant can be renewed. Although a warrant can be renewed indefinitely, the Secretary of State himself must authorise any renewal and, upon such authorisation, must again satisfy himself that the warrant remains necessary on the grounds stipulated in section 5(3). In the context of national security and serious crime, the Court observes that the scale of the criminal activities involved is such that their planning often takes some time. Subsequent investigations may also be of some duration, in light of the general complexity of such cases and the numbers of individuals involved. The Court is therefore of the view that the overall duration of any interception measures will depend on the complexity and duration of the investigation in question and, provided that adequate safeguards exist, it is not unreasonable to leave this matter for the discretion of the relevant domestic authorities. The Code explains that the person seeking the renewal must make an application to the Secretary of State providing an update and assessing the value of the interception operation to date. He must specifically address why he considers that the warrant remains necessary on section 5(3) grounds. Further, under section 9(3) RIPA, the Secretary of State is obliged to cancel a warrant where he is satisfied that the warrant is no longer necessary on section 5(3) grounds. There is also provision in the Act for specific factors in the schedule to the warrant to be deleted where the Secretary of State considers that they are no longer relevant for identifying communications from or to the interception subject. The Code advises that the duty on the Secretary of State to cancel warrants which are no longer necessary means, in practice, that intercepting agencies must keep their warrants under continuous review. The Court concludes that the provisions on duration, renewal and cancellation are sufficiently clear.

***Iordachi and Others v Moldova*, App No 25198/02, Judgment, European Court of Human Rights (10 February 2009)**

44. Still, the nature of the offences which may give rise to the issue of an interception warrant is not, in the Court's opinion, sufficiently clearly defined in the impugned legislation. In particular, the Court notes that more than one half of the offences provided for in the Criminal Code fall within the category of offences eligible for interception warrants. Moreover, the Court is concerned by the fact that the impugned legislation does not appear to define sufficiently clearly the categories of persons liable to have their telephones tapped. It notes that Article 156 § 1 of the Criminal Code uses very general language when referring to such persons and states that the measure of interception may be used in respect of a suspect, defendant or other person involved in a criminal offence. No explanation has been given as to who exactly falls within the category of "other person involved in a criminal offence.

45. The Court further notes that the legislation in question does not provide for a clear limitation in time of a measure authorising interception of telephone communications. While the Criminal Code imposes a limitation of six months, there are no provisions under the impugned legislation which would prevent the prosecution authorities from seeking and obtaining a new interception warrant after the expiry of the statutory six months' period.

46. Moreover, it is unclear under the impugned legislation who – and under what circumstances – risks having the measure applied to him or her in the interests of, for instance, protection of health or morals or in the interests of others. While enumerating in section 6 and in Article 156 § 1 the circumstances in which tapping is susceptible of being applied, the Law on Operational Investigative Activities and the Code of Criminal Procedure fails, nevertheless, to define "national security", "public order", "protection of health", "protection of morals", "protection of the rights and interests of others", "interests of ... the economic situation of the country" or "maintenance of legal order" for the purposes of interception of telephone communications. Nor does the legislation specify the circumstances in which an individual may be at risk of having his telephone communications intercepted on any of those grounds.

***S. and Marper v The United Kingdom*, Apps Nos 30562/04 and 30566/04, Judgment, European Court of Human Rights (4 December 2008)**

96. The level of precision required of domestic legislation – which cannot in any case provide for every eventuality – depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed.

***Liberty and Others v The United Kingdom*, App No 58243/00, Judgment, European Court of Human Rights (1 July 2008)**

60. […] [The Government responded] that although the scope of the executive's discretion to carry out surveillance had to be indicated in legislation, "the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law".

61. The Court observes, first, that the above passage from Malone was itself a reference to *Silver and Others*. There the Court accepted that administrative Orders and Instructions, which set out the detail of the scheme for screening prisoners' letters but did not have the force of law, could be taken into account in assessing whether the criterion of foreseeability was satisfied in the application of the relevant primary and secondary legislation, but only to "the admittedly limited extent to which those concerned were made sufficiently aware of their contents". It was only on this basis – that the content of the Orders and Instructions were made known to the prisoners – that the Court was able to reject the applicants' contention that the conditions and procedures governing interferences with correspondence, and in particular the directives set out in the Orders and Instructions, should be contained in the substantive law itself.

63. It is true that the above requirements were first developed by the Court in connection with measures of surveillance targeted at specific individuals or addresses (the equivalent, within the United Kingdom, of the section 3(1) regime). However, the *Weber and Saravia* case was itself concerned with generalised "strategic monitoring", rather than the monitoring of individuals. The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other. […]

***Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, App No 62540/00, Judgment, European Court of Human Rights (28 June 2007)**

75. In the context of covert measures of surveillance, the law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence. In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.

***Kopp v Switzerland*, App No 23224/94, Judgment, European Court of Human Rights (25 March 1998)**

72. The Court, however, is not persuaded by these arguments. Firstly, it is not for the Court to speculate as to the capacity in which Mr Kopp had had his telephones tapped, since he was a lawyer and all his law firm's telephone lines had been monitored. Secondly, tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated. In that connection, the Court by no means seeks to minimise the value of some of the safeguards built into the law, such as the requirement at the relevant stage of the proceedings that the prosecuting authorities' telephone-tapping order must be approved by the President of the Indictment Division, who is an independent judge, or the fact that the applicant was officially informed that his telephone calls had been intercepted.

***Kruslin v France*, App No 11801/85, Judgment, European Court of Human Rights (24 April 1990)**

28. The Delegate of the Commission considered that in the case of the Continental countries, including France, only a substantive enactment of general application - whether or not passed by Parliament - could amount to a "law" for the purposes of Article 8 § 2 (art. 8-2) of the Convention. Admittedly the Court had held that "the word 'law' in the expression 'prescribed by law' cover[ed] not only statute but also unwritten law", but in those instances the Court was, so the Delegate maintained, thinking only of the common-law system. That system, however, was radically different from, in particular, the French system. In the latter, case-law was undoubtedly a very important source of law, but a secondary one, whereas by "law" the Convention meant a primary source.

29. […] In relation to paragraph 2 of Article 8 (art. 8-2) of the Convention and other similar clauses, the Court has always understood the term "law" in its "substantive" sense, not its "formal" one; it has included both enactments of lower rank than and unwritten law. The *Sunday Times*, *Dudgeon*, and *Chappell* Judgments admittedly concerned the United Kingdom, but it would be wrong to exaggerate the distinction between common-law countries and Continental countries, as the Government rightly pointed out... In a sphere covered by the written law, the "law" is the enactment in force as the competent courts have interpreted it in the light, if necessary, of any new practical developments.

31. The Government submitted that the Court must be careful not to rule on whether French legislation conformed to the Convention in the abstract and not to give a decision based on legislative policy. The Court was therefore not concerned, they said, with matters irrelevant to Mr Kruslin's case, such as the possibility of telephone tapping in relation to minor offences or the fact that there was no requirement that an individual whose telephone had been monitored should be so informed after the event where proceedings had not in the end been taken against him. Such matters were in reality connected with the condition of "necessity in a democratic society", fulfilment of which had to be reviewed in concrete terms, in the light of the particular circumstances of each case.

32. The Court is not persuaded by this argument. Since it must ascertain whether the interference complained of was "in accordance with the law", it must inevitably assess the relevant French "law" in force at the time in relation to the requirements of the fundamental principle of the rule of law. Such a review necessarily entails some degree of abstraction. It is none the less concerned with the "quality" of the national legal rules applicable to Mr Kruslin in the instant case.

***Leander v Sweden*, App No 9248/81, Judgment, European Court of Human Rights (26 March 1987)**

50. The expression "in accordance with the law" in paragraph 2 of Article 8 (art. 8-2) requires, to begin with, that the interference must have some basis in domestic law. Compliance with domestic law, however, does not suffice: the law in question must be accessible to the individual concerned and its consequences for him must also be foreseeable.

51. However, the requirement of foreseeability in the special context of secret controls of staff in sectors affecting national security cannot be the same as in many other fields. Thus, it cannot mean that an individual should be enabled to foresee precisely what checks will be made in his regard by the Swedish special police service in its efforts to protect national security. Nevertheless, in a system applicable to citizens generally, as under the Personnel Control Ordinance, the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life. In assessing whether the criterion of foreseeability is satisfied, account may be taken also of instructions or administrative practices which do not have the status of substantive law, in so far as those concerned are made sufficiently aware of their contents. In addition, where the implementation of the law consists of secret measures, not open to scrutiny by the individuals concerned or by the public at large, the law itself, as opposed to the accompanying administrative practice, must indicate the scope of any discretion conferred on the competent authority with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.

***Escher et al. v Brazil*, Inter-American Court of Human Rights, Judgment (on Preliminary Objections, Merits, Reparations, and Costs), Series C No 200 (6 July 2009)**

118. The Commission alleged that although the laws that authorize the interception and monitoring of telephone or any other type of communications were formulated to combat crime, they can become an instrument for spying and harassment if they are interpreted and applied improperly. Hence, owing to the inherent danger of abuse in any monitoring system, this measure must be based on especially precise legislation with clear, detailed rules. The American Convention protects the confidentiality and inviolability of communications from any kind of arbitrary or abusive interference from the State or individuals; consequently, the surveillance, intervention, recording and dissemination of such communications is prohibited, except in the cases established by law that are adapted to the objects and purposes of the American Convention.

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet OEA/Ser.L/V/II. CIDH/RELE/INF.11/13 (31 December 2013)

155. [...] the existence of a law is not enough for a program to be legitimate. As previously mentioned, vague or ambiguous legal provisions that grant very broad discretionary powers are incompatible with the American Convention, because they can serve as the basis for potential arbitrary acts that translate into violations of the right to privacy or the right to freedom of thought and expression guaranteed by the Convention.

156. The laws that authorize the interception of communications must establish clearly and precisely the reasons the State can invoke to request that interception, which can only be authorized by a judge. Additionally, must be established by law safeguards pertaining to the nature, scope, and duration of the surveillance measures; the facts that could justify these measures, and the authorities competent to authorize them, carry them out, and supervise them. The law must be clear with regard to the possible remedies for abuses committed in the exercise of those powers.

C. THE PRINCIPLE OF NECESSITY

The review of pronouncements by different human rights monitoring mechanisms shows that there are significant overlaps in references to the principles of legality, necessity and proportionality. Whether an appraisal is made within the test of necessity or proportionality will also often depend on the particular approach adopted by the court in question. This is particularly the case for the principles of necessity and proportionality, as well as whether the aim pursued is an element in the assessment of necessity, or of legality. It may therefore be pertinent to also consult other sub-chapters. Reference to the principle of necessity within the broader framework of principles governing surveillance can be found in the introductory sub-section A.

Report of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/48/31 (13 September 2021)

39. […] States should also determine if less invasive approaches could achieve the same results with the same effectiveness; if so, those measures need to be taken. The High Commissioner has already outlined such necessary limitations and safeguards in the context of surveillance by intelligence agencies and law enforcement. It should be noted that the necessity and proportionality tests can also lead to the conclusion that certain measures must not be taken. For example, requirements of blanket, indiscriminate retention of communications data imposed on telecommunications and other companies would fail the proportionality test. […] Moreover, it is crucial that measures are not assessed in isolation, but that the cumulative effects of distinct but interacting measures are properly taken into account. […]

Report of the United Nations High Commissioner for Human Rights, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests, UN Doc A/HRC/44/24 (24 June 2020)

25. Similarly, the Special Rapporteur on the right to freedom of opinion and expression has called for strict limitations on restrictions to encryption and anonymity in order to ensure compliance with the principles of legality, necessity, proportionality and legitimacy. Such restrictions are often used by law enforcement and intelligence agencies as quick reactions to terrorism, while failing to meet imperatives of necessity and proportionality, and consequently undermining trust in the rule of law. Other experts have recalled the importance of judicial control and proportionality when anonymity is lifted.

35. Audiovisual recording and facial recognition techniques should only be used when such measures meet the three-part test of legality, necessity and proportionality. The possibility that recourse to facial recognition technology during peaceful protests could ever meet the test of necessity and proportionality, given its intrusiveness and serious chilling effects, has been questioned. Authorities should generally refrain from recording assembly participants. As required by the need to show proportionality, exceptions should only be considered when there are concrete indications that serious criminal offences are actually taking place or that there is cause to suspect imminent and serious criminal behaviour, such as violence or the use of firearms. Existing recordings should only be used for the identification of assembly participants who are suspects of serious crimes.

53. In this context, the High Commissioner recommends that States: (d) Ensure that any interference with the right to privacy, including by communications surveillance and intelligence-

sharing, complies with international human rights law, including the principles of legality, necessity and proportionality;

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

24. […] (b) Necessity and proportionality: the State has the burden of proving a direct and immediate connection between the expression and the threat and that the restriction it seeks to impose is the least intrusive instrument among those that might achieve the same protective function […].

50. As a primary step, Governments deploying surveillance tools must ensure that they do so in accordance with a domestic legal framework that meets the standards required by international human rights law…. To be compliant with those standards, national laws must: (b) Require that any legislation governing surveillance…only be applied when necessary and proportionate to achieve one of the legitimate objectives enumerated in article 19 (3) of the International Covenant on Civil and Political Rights;

66. For States: (b) States that purchase or use surveillance technologies ("purchasing States") should ensure that domestic laws permit their use only in accordance with the human rights standards of legality, necessity and legitimacy of objectives, and establish legal mechanisms of redress consistent with their obligation to provide victims of surveillance-related abuses with an effective remedy;

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/29/32 (22 May 2015)

34. Third, the State must show that any restriction on encryption or anonymity is "necessary" to achieve the legitimate objective. The European Court of Human Rights has concluded appropriately that the word "necessary" in article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms means that the restriction must be something more than "useful," "reasonable" or "desirable". Once the legitimate objective has been achieved, the restriction may no longer be applied. Given the fundamental rights at issue, limitations should be subject to independent and impartial judicial authority, in particular to preserve the due process rights of individuals. […]

60. States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression. Blanket prohibitions fail to be necessary and proportionate. States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows.

***P.N. v Germany*, App No 74440/17, Judgment, European Court of Human Rights (11 June 2020)**

69. […] the interference in question can be considered "necessary in a democratic society", which means that it must answer a "pressing social need" and, in particular, be proportionate to the legitimate aim pursued, and that the reasons adduced by the national authorities to justify it must be "relevant and sufficient" […].

71. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored, and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those

data are stored […].

76. […] the police and the domestic courts had to take into account the nature and gravity of the offences previously committed by the applicant in their decision to collect and store identification data from him […].

79. As the domestic authorities stressed, these last proceedings were taken into account in their preventive assessment of whether it was likely that the applicant might be suspected of an offence in the future. The Court can therefore accept that these discontinued proceedings, none of which ended with the domestic authorities' finding that the applicant was innocent and in the absence of any indication that these proceedings had been instituted arbitrarily, were also relevant, to a very limited extent, in that assessment.

84. In its assessment of the proportionality of the impugned measure, the Court further considers it an important element that the collection and retention of the identification data here at issue – photographs, fingerprints and palm prints and a description of the person – constitute a less intrusive interference with the applicant's right to respect for his private life notably than the collection of cellular samples and the retention of DNA profiles, which contain considerably more sensitive information.

85. […] Data must be deleted if they are no longer necessary for the purposes of police work. The purposes of the storage, as well as the type and significance of the reason for the storage, must be taken into account in the assessment thereof. In a case like that of the applicant – an adult offender whose offences were neither of minor nor of special significance as defined by the relevant directive – personal data are to be deleted, as a rule, after five years.

87. In view of the relatively limited intrusiveness and duration of the collection as such of the identification data in question and the limited effect of the retention of the data in an internal police database on the applicant's daily life, the Court, having regard to the material before it, further considers that the applicant failed to substantiate that his state of health […] has been affected by the stress and unease caused by the impugned measure.

88. It is also apparent from the foregoing considerations that there is a possibility of review – by the police authorities, subject to judicial review […] – of the necessity of further retaining the data in question. […] There is nothing to indicate that this review does not, in practice, allow the deletion of the identification data if they are no longer needed for the purpose for which they were obtained.

89. The Court further notes that there is nothing to indicate, and the applicant has not argued, that the identification data taken from him and stored by the police were insufficiently protected against abuse such as unauthorised access or dissemination.

90. Having regard to the foregoing considerations, the Court concludes that the reasons adduced by the national authorities to justify the interference with the applicant's right to respect for his private life by the taking and storage of personal data from him were "relevant and sufficient".

***Szabó and Vissy v Hungary*, App No 37138/14, Judgment, European Court of Human Rights (12 January 2016)**

21. [The] Judgment use[s] a "strict necessity" test and refer it to two purposes: the safeguarding of democratic institutions and the acquiring of vital intelligence in an individual operation. His creative rephrasing of the legal test raises several problems. Firstly, it is a stricter criterion than that in paragraphs 233 and 236 of Roman Zakharov. Secondly, it does not match the looser criterion for the degree of suspicion of involvement in the offences or activities being monitored. It

is logically inconsistent that the same Judgment imposes a "strict necessity" test for the determination of the surveillance measure, but at the same time accepts a very loose criterion for the degree of suspicion of involvement in the offences or activities being monitored, as demonstrated above. It is logically incoherent to criticise the overly broad text of the Hungarian law when it refers to the "persons concerned identified as a range of persons" and yet to accept the linguistically vague and legally imprecise "individual suspicion" test to ground the applicability of a surveillance measure. Thirdly, the Chamber did not clarify in what the "strict necessity test" consists, having merely linked the test to the purposes pursued. Nowhere does the Judgment clarify that the necessity test warrants that any surveillance operation be ordered only if the establishment of the facts by other less intrusive methods has proven unsuccessful or, exceptionally, if other less intrusive methods are deemed unlikely to succeed.

71. […] the mere requirement for the authorities to give reasons for the request, arguing for the necessity of secret surveillance, falls short of an assessment of strict necessity. There is no legal safeguard requiring TEK to produce supportive materials or, in particular, a sufficient factual basis for the application of secret intelligence gathering measures which would enable the evaluation of necessity of the proposed measure – and this on the basis of an individual suspicion regarding the target person. For the Court, only such information would allow the authorising authority to perform an appropriate proportionality test.

72. Quite apart from what transpires from section 53(2) of the National Security Act, the Court recalls at this point that in *Klass and Others* it held that "powers of secret surveillance of citizens [...] are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions". Admittedly, the expression "strictly necessary" represents at first glance a test different from the one prescribed by the wording of paragraph 2 of Article 8, that is, "necessary in a democratic society".

73. However, given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity" in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. The Court notes that both the Court of Justice of the European Union and the United Nations Special Rapporteur require secret surveillance measures to answer to strict necessity – an approach it considers convenient to endorse.

***Weber and Saravia v Germany*, App No 54934/00, Decision, European Court of Human Rights (29 June 2006)**

104. The Court shares the Government's view that the aim of the impugned provisions of the amended G10 Act was indeed to safeguard national security and/or to prevent crime, which are legitimate aims within the meaning of Article 8 § 2. It does not, therefore, deem it necessary to decide whether the further purposes cited by the Government were also relevant.

105. It remains to be ascertained whether the impugned interferences were "necessary in a democratic society" in order to achieve these aims.

106. The Court reiterates that when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interferences with an applicant's right to respect for his or her private life, it has consistently

recognized that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aims of protecting national security. Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.

Annual Report of the Inter-American Commission on Human Rights 2020, Volume II – Annual Report of the Office of the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II Doc 28 (30 March 2021)

175. The privacy of information in the digital age must be preserved. To this end, states must protect anonymity, as well as the encryption and inviolability of communications. They must set limits on the power to monitor private communications and establish the necessity and proportionality of such surveillance in accordance with individual human rights and the principles of international law. Provisions on the mandatory registration of SIM cards and cell phones and any other measure that could lead to intercepting communications outside the limits permitted by international law must also be legitimate and must not violate the confidentiality of sources.

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

24. […] Governments seeking to limit encryption have often failed to show that the restrictions they would impose are necessary to meet a particular legitimate interest, given the availability of various other tools and approaches that provide the information needed for specific law enforcement or other legitimate purposes. Such alternative measures include improved, better-resourced traditional policing, undercover operations, metadata analysis and strengthened international police cooperation.

50. Legitimate goals: there is no doubt that public surveillance can serve a broad range of legitimate goals, for example the protection of people's lives or bodily integrity and the security of critical infrastructure. Regrettably, public surveillance is routinely conducted for aims that are not permissible under international human rights law. […]

57. […] OHCHR recommends that States: (d) Avoid general privacy-intrusive monitoring of public spaces and ensure that all public surveillance measures are strictly necessary and proportionate for achieving important legitimate objectives, including by strictly limiting their location and time, as well as the duration of data storage, the purpose of data use and access to data; […]

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

23. […] The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. […].

25. […] Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being

addressed. Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate.

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/43/52 (24 March 2020)

42. States and non-State actors should ensure the highest attainable standard of data protection for all individuals, regardless of their gender, by: (g) Employing the principles of data minimization, necessity and proportionality when aggregating gender data so that only the minimum necessary level of detail is included in a data set to achieve the intended positive outcome of the use of the data; (…)

52. States and non-State actors should: (a) Protect the privacy of digital communications and enjoyment of the right to privacy by all individuals, regardless of their gender, by promoting tools such as encryption; (b) Ensure that restrictions to the right to privacy, including through mass or targeted surveillance, requests for personal data or limitations on the use of encryption, pseudonymity and anonymity tools: (i) Are on a case-specific basis; (ii) Do not discriminate on the basis of gender or other factors, such as indigeneity; (iii) Are reasonable, necessary and proportionate as required by law for a legitimate purpose and ordered only by a court.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/32/38 (11 May 2016)

85. States bear a primary responsibility to protect and respect the right to exercise freedom of opinion and expression. In the information and communication technology context, this means that States must not require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extralegal means. Any demands, requests and other measures to take down digital content or access customer information must be based on validly enacted law, subject to external and independent oversight, and demonstrate a necessary and proportionate means of achieving one or more aims under article 19 (3) of the International Covenant on Civil and Political Rights. Particularly in the context of regulating the private sector, State laws and policies must be transparently adopted and implemented [...]

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/23/40 (17 April 2013)

83. Legal frameworks must ensure that communications surveillances measures: ... (b) are strictly and demonstrably necessary to achieve a legitimate aim.

Concluding Observations on the Seventh Periodic Report of Germany, Human Rights Committee, UN Doc CCPR/C/DEU/CO/7 (11 November 2021)

42. The Committee is concerned about the wide reaching powers of surveillance, including online surveillance and the hacking of encrypted communications data during criminal investigations. […]

***Toonen v Australia*, Comm No 488/1992, Human Rights Committee, UN Doc CCPR/C/50/D/488/1992 (31 March 1994)**

8.3 [...] any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case.

***Škoberne v Slovenia*, App No 19920/20, Judgment, European Court of Human Rights (15 February 2024)**

124. As to the question of whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aims of, *inter alia*, protecting national security or preventing and prosecuting criminal offences. However, this margin is subject to European supervision embracing both legislation and decisions applying it, and considering all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by national law (see *Roman Zakharov*, § 232, and *Breyer*, § 79, both cited above).

***N.F. and Others v Russia*, Apps Nos 3537/15 and 8 others, Judgment, European Court of Human Rights (12 September 2023)**

45. An interference will be considered "necessary in a democratic society" in order to achieve a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient". While it is for the national authorities to make the initial assessment in all these respects, the final evaluation of whether the interference is necessary remains subject to review by the Court for conformity with the requirements of the Convention (see *S. and Marper*, cited above, § 101). […]

***Glukhin v Russia*, App No 11519/20, Judgment, European Court of Human Rights (04 July 2023)**

86. In determining whether the processing of the applicant's personal data was "necessary in a democratic society", the Court will first assess the level of the actual interference with the right to respect for private life (see *N. v. Germany*, cited above, §§ 73 and 84). It notes that the police collected and stored the applicant's digital images and used them to extract and process the applicant's biometric personal data with the aid of facial recognition technology: first, to identify him from the photographs and the video published on Telegram and, secondly, to locate and arrest him while he was travelling on the Moscow underground. The Court considers these measures to be particularly intrusive, especially in so far as live facial recognition technology is concerned (see paragraph 37 above). A high level of justification is therefore required in order for them to be considered "necessary in a democratic society", with the highest level of justification required for the use of live facial recognition technology. Moreover, the personal data processed contained information about the applicant's participation in a peaceful protest and therefore revealed his political opinion. They accordingly fell in the special categories of sensitive data attracting a heightened level of protection (see paragraph 76 above).

87. In the assessment of the "necessity in a democratic society" of the processing of personal data in the context of investigations, the nature and gravity of the offences in question is one of the elements to be taken into account (see, mutatis mutandis, *N. v. Germany*, cited above, § 72). The domestic law permits the processing of biometric personal data in connection with the investigation and prosecution of any offence, irrespective of its nature and gravity.

88. The Court observes that the applicant was prosecuted for a minor offence consisting of holding a solo demonstration without a prior notification – an offence classified as administrative rather than criminal under the domestic law. He was never accused of committing any reprehensible acts during his demonstration, such as the obstruction of traffic, damage to property or acts of violence. It was never claimed that his actions presented any danger to public order or transport safety. The Court has already found that the administrative-offence proceedings against the applicant breached his right to freedom of expression (see paragraph 57 above). It considers that the use of highly intrusive

facial recognition technology to identify and arrest participants of peaceful protest actions could have a chilling effect in regard of the rights to freedom of expression and assembly.

89. In such circumstances, the use of facial recognition technology to identify the applicant from the photographs and the video published on Telegram – and a fortiori the use of live facial recognition technology to locate and arrest him while he was travelling on the Moscow underground – did not correspond to a "pressing social need".

90. In the light of all the above considerations the Court concludes that the use of highly intrusive facial recognition technology in the context of the applicant exercising his Convention right to freedom of expression is incompatible with the ideals and values of a democratic society governed by the rule of law, which the Convention was designed to maintain and promote. The processing of the applicant's personal data using facial recognition technology in the framework of administrative offence proceedings – first, to identify him from the photographs and the video published on Telegram and, secondly, to locate and arrest him while he was travelling on the Moscow underground – cannot be regarded as "necessary in a democratic society".

***Svetova and Others v Russia*, App No 54714/17, Judgment, European Court of Human Rights (24 January 2023)**

40. The Court further notes that the search warrant was issued fourteen years after the opening of a criminal case against the third parties and was executed forty days after it had been issued. Such a wide time frame, in the absence of any explanation, makes doubtful its usefulness for the investigation.

41. The Court observes that in previous Russian cases it was the vagueness and excessively broad terms of search warrants that were considered to constitute the decisive element for the finding of a violation of Article 8, as they gave the authority executing them unrestricted discretion in determining the scope of the search (see *Aleksanyan v. Russia*, no. 46468/06, § 216, 22 December 2008; *Kolesnichenko v. Russia*, no. 19856/04, § 33, 9 April 2009; and *Misan*, cited above, § 60).

42. In the instant case, the search record, which appears to reflect the language of the search warrant, indicated that the purpose of the search was to discover and seize any documents containing information about funds received from the owners of several offshore companies, including Mr Khodorkovskiy. In light of the extremely wide time frame of the criminal proceedings and the fact that the applicants were not suspected of any criminal behaviour, the Court considers that these are general and broad terms which gave the police unrestricted discretion in determining which items and documents were to be seized (compare *Misan*, cited above, § 61). On the basis of that overly broad scope, the investigator removed multiple personal items belonging to the applicants (see paragraph 18 above). Such indiscriminate seizure cannot be considered "necessary in a democratic society".

***Big Brother Watch and Others v The United Kingdom*, Apps Nos 58170/13, 62322/14 and 24960/15, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

347. […] While Article 8 of the Convention does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats, and States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary, for these purposes, in operating such a system the margin of appreciation afforded to them must be narrower and a number of safeguards will have to be present. […]

350. Therefore, in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent

authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review. In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime (see also the report of the Venice Commission, at paragraph 197 above, which similarly found that two of the most significant safeguards in a bulk interception regime were the authorisation and oversight of the process).

355. […] The use of every such selector must be justified – with regard to the principles of necessity and proportionality – by the intelligence services and that justification should be scrupulously recorded and be subject to a process of prior internal authorisation providing for separate and objective verification of whether the justification conforms to the aforementioned principles.

356. […] the supervising body should be in a position to assess the necessity and proportionality of the action being taken, having due regard to the corresponding level of intrusion into the Convention rights of the persons likely to be affected. […]

***Centrum för Rättvisa v Sweden*, App No 35252/08, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

264. Therefore, in order to minimise the risk of the bulk interception being abused, the Court considers that the process must be subject to "end- to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the bulk operation are being defined; and that the operation should be subject to supervision and independent *ex post facto* review. In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime (see also the report of the Venice Commission, at paragraph 86 above, which similarly found that two of the most significant safeguards in a bulk interception regime were the authorisation and oversight of the process)."

***Yunusova and Yunusov v Azerbaijan (No 2)*, App No 68817/14, Judgment, European Court of Human Rights (16 July 2020)**

154. However, in the Court's view, the above unspecified "emerging necessity" within the criminal case against R.M. and the mere fact that the latter was in close relationship with the applicants and had cooperated with the Association cannot be considered, in the absence of any concrete purpose of those measures, as reasonable grounds for suspecting that evidence relevant for the investigation of that criminal case might have been found as a result of those searches. […]

155. […] the Court finds that the Government failed to convincingly demonstrate that the authorities had been guided by the legitimate aims relied on, that is to say the investigation of the criminal case against R.M. and the protection of national security.

157. Accordingly, the Court finds that, in the particular circumstances of the present case, the search and seizure at the applicants' home and the Association's offices as well as the inspection of the applicants' luggage and handbags at the airport and seizure of various objects and documents, including the applicants' passports, did not pursue any of the legitimate aims enumerated in paragraph 2 of Article 8.

158. Where it has been shown that an interference did not pursue a "legitimate aim" it is not necessary to investigate whether it was "necessary in a democratic society" […]."

***Gaughran v The United Kingdom*, App No 45245/15, Judgment, European Court of Human Rights (13 February 2020)**

77. A margin of appreciation must be left to the competent national authorities in this assessment. The breadth of this margin varies and depends on a number of factors, including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference. The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights. Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State will be restricted. Where, however, there is no consensus within the member States of the Council of Europe, either as to the relative importance of the interest at stake or as to how best to protect it, the margin will be wider.

80. […] for both fingerprints and photographs the majority of States surveyed have put in place regimes with defined retention periods.

81. […] The Court recalls that when considering the nature of the interference with privacy occasioned by the retention of DNA profiles, it has observed that the use of DNA profiles for familial searching with a view to identifying a possible genetic relationship between individuals is of a highly sensitive nature and there is a need for very strict controls in this respect. […]

84. In light of the above, the Court cannot conclude that the State's margin of appreciation is widened in the present case to the extent claimed by the Government. The United Kingdom is one of the few Council of Europe jurisdictions to permit indefinite retention of DNA profiles, fingerprints and photographs of convicted persons. The degree of consensus existing amongst Contracting States has narrowed the margin of appreciation available to the respondent State in particular in respect of the retention of DNA profiles […].

***Hambardzumyan v Armenia*, App No 43478/11, Judgment, European Court of Human Rights (5 December 2019)**

61. As to the question of whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court reiterates that powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions. In practice, this means that there must be adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law (see *Kennedy*, cited above, § 153).

62. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society". In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded (see *Kvasnica v. Slovakia*, no. 72094/01, § 80, 9 June 2009; and Kennedy, cited above, § 154).

***Bosak and Others v Croatia*, Apps Nos 40429/14 and 3 others, Judgment, European Court of Human Rights (6 June 2019)**

45. […] [the secret surveillance orders] were essentially based on a statement referring to the existence of the competent prosecutor's request for the use of secret surveillance and the statutory phrase that "the investigation could not be conducted by other means". They did not, however, provide adequate reasoning as to the particular circumstances of the case, and in particular reasons why the investigation could not be conducted by other, less intrusive, means […].

***Liblik and Others v Estonia*, Apps Nos 173/15 and 5 others, Judgment, European Court of Human Rights (28 May 2019)**

131. This in particular bears significance as to the question of whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, since the Court has held that powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions. In assessing the existence and extent of such necessity, the Contracting States enjoy a certain margin of appreciation. However, this margin is subject to European supervision embracing both legislation and decisions applying it (see *Roman Zakharov*, cited above, §232).

***Catt v The United Kingdom*, App No 43514/15, Judgment, European Court of Human Rights (24 January 2019)**

109. The Court has set out on many occasions the elements to be taken into account when considering whether an interference in an applicant's Article 8 rights was necessary and therefore justified. It will be necessary in a democratic society if it answers to a "pressing social need", if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are relevant and sufficient". A margin of appreciation must be left to the competent national authorities in this assessment.

***Ivashchenko v Russia*, App No 61064/10, Judgment, European Court of Human Rights (13 February 2018)**

75. The above considerations under the heading of "quality of law" may overlap with similar issues analysed under the heading of "necessary in a democratic society". The Court reiterates that where a wide margin of appreciation is afforded to the national authorities, the procedural safeguards available to the individual will be especially material in determining whether the respondent State has, when fixing the regulatory framework, remained within its margin of appreciation. In particular, the Court must examine whether the decision-making process leading to measures of interference was fair and such as to afford due respect to the interests safeguarded to the individual by the Convention. […]

Dudchenko v Russia*, App No 37717/05, Judgment, European Court of Human Rights (7 November 2017)

92. An interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient". While it is for the national authorities to make the initial assessment in all these respects, the final evaluation of whether the interference is necessary remains subject to review by the Court for conformity with the requirements of the Convention. In the context of covert surveillance, the assessment depends on all the circumstances of the case, such as the nature, scope and duration of the surveillance measures, the grounds for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. […]

95. Although the applicant has not complained that the quality of the domestic law fell short of the Convention standards, when examining whether the interference complained of was "in accordance with the law", the Court must assess the quality of the relevant domestic law in relation to the requirements of the fundamental principle of the rule of law. The Court notes in this connection that in the case of *Roman Zakharov Russia* it has already found that Russian law does not meet the "quality of law" requirement because the legal provisions governing the interception of communications do not provide for adequate and effective guarantees against arbitrariness and the risk of abuse. They are therefore incapable of keeping the "interference" to what is "necessary in a democratic society". […]

96. In the *Roman Zakharov* case the Court has found, in particular, that the judicial authorisation

procedures provided for by Russian law are not capable of ensuring that covert surveillance measures are not ordered haphazardly, irregularly or without due and proper consideration. In particular, the CCrP does not instruct judges ordering covert surveillance measures to verify the existence of a "reasonable suspicion" against the person concerned or to apply the "necessity" and "proportionality" tests. The Court has also found it established, on the basis of evidence submitted by the parties, that in their everyday practice the Russian courts do not verify whether there is a "reasonable suspicion" against the person concerned and do not apply the "necessity" and "proportionality" tests. […]

98. Furthermore, there is no indication in the text of the surveillance authorisation that the court applied the test of "necessity in a democratic society", and in particular assessed whether the surveillance measures carried out against the applicant were proportionate to any legitimate aim pursued. In particular, the court failed to recognise that the case involved a conflict between the right to respect for private life and correspondence and other legitimate interests and to perform a balancing exercise. The only reason advanced by the court to justify the surveillance measures was that it "seem[ed] impossible to obtain the information necessary to expose [the applicant's] unlawful activities by overt investigation", without explaining how it had come to that conclusion. The Court does not consider that such a vague and unsubstantiated statement was sufficient to justify the decision to authorise a lengthy (180 days) covert surveillance operation, which entailed a serious interference with the right to respect for the applicant's private life and correspondence.

99. To sum up, the Court finds that the domestic court that authorised covert surveillance measures against the applicant […] did not apply the "necessity in a democratic society" and "proportionality" tests.

**See also paras 98-100 repeated in Moskalev v Russia, App No 44045/05, Judgment, European Court of Human Rights (7 November 2017), paras 36-45; Zubkov and others v Russia, App No 29431/05 and 2 others, Judgment, European Court of Human Rights (7 November 2017), paras 123-128*

***Konstantin Moskalev v Russia*, App No 59589/10, Judgment, European Court of Human Rights (7 November 2017)**

48. An interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient". While it is for the national authorities to make the initial assessment in all these respects, the final evaluation of whether the interference is necessary remains subject to review by the Court for conformity with the requirements of the Convention. In the context of covert surveillance the assessment depends on all the circumstances of the case, such as the nature, scope and duration of the covert surveillance measures, the grounds for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. […]

***Roman Zakharov v Russia*, App No 47143/06, Judgment, European Court of Human Rights (4 December 2015)**

232. As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse. The

assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society". […]

236. In cases where the legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question whether the "necessity" test has been complied with and it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements. The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards and guarantees against abuse.

237. It has not been disputed by the parties that interceptions of mobile telephone communications have a basis in the domestic law. They are governed, in particular, by the CCrP and the OSAA, as well as by the Communications Act and the Orders issued by the Ministry of Communications. Furthermore, the Court considers it clear that the surveillance measures permitted by Russian law pursue the legitimate aims of the protection of national security and public safety, the prevention of crime and the protection of the economic well-being of the country.

***Dragojević v Croatia*, App No 68955/11, Judgment, European Court of Human Rights (15 January 2015)**

83. […] in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist guarantees against abuse which are adequate and effective. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.

84. This in particular bears significance as to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, since the Court has held that powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions. In assessing the existence and extent of such necessity the Contracting States enjoy a certain margin of appreciation but this margin is subject to European supervision. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society". In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. […]

89. […] the central question for the Court to determine is whether the relevant domestic law, including the way in which it was interpreted by the domestic courts, indicated with reasonable clarity the scope and manner of exercise of the discretion conferred on the public authorities, and in particular whether the domestic system of secret surveillance, as applied by the domestic authorities, afforded adequate safeguards against various possible abuses. Since the existence of adequate safeguards against abuse is a matter closely related to the question whether the "necessity" test was complied with in this case, the Court will address both the requirement that the interference be "in accordance with the law" and that it be "necessary" […]

97. It follows from the foregoing that whereas the Code of Criminal Procedure expressly envisaged prior judicial scrutiny and detailed reasons when authorising secret surveillance orders, in order for such measures to be put in place, the national courts introduced the possibility of retrospective

justification of their use, even where the statutory requirement of prior judicial scrutiny and detailed reasons in the authorisation was not complied with. In an area as sensitive as the use of secret surveillance, which is tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions, the Court has difficulty in accepting this situation created by the national courts […]

98. Moreover, the Court considers that in a situation where the legislature envisaged prior detailed judicial scrutiny of the proportionality of the use of secret surveillance measures, a circumvention of this requirement by retrospective justification, introduced by the courts, can hardly provide adequate and sufficient safeguards against potential abuse since it opens the door to arbitrariness by allowing the implementation of secret surveillance contrary to the procedure envisaged by the relevant law.

***Rotaru v Romania*, App No 28341/95, Judgment, European Court of Human Rights (4 May 2000)**

47. The cardinal issue that arises is whether the interference so found is justifiable under paragraph 2 of Article 8. That paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be interpreted narrowly. While the Court recognises that intelligence services may legitimately exist in a democratic society, it reiterates that powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.

***Leander v Sweden*, App No 9248/81, Judgment, European Court of Human Rights (26 March 1987)**

58. The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued.

59. However, the Court recognises that the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved. In the instant case, the interest of the respondent State in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his private life. There can be no doubt as to the necessity, for the purpose of protecting national security, for the Contracting States to have laws granting the competent domestic authorities power, firstly, to collect and store in registers not accessible to the public information on persons and, secondly, to use this information when assessing the suitability of candidates for employment in posts of importance for national security.

***Malone v The United Kingdom*, App No 8691/79, Judgment, European Court of Human Rights (2 August 1984)**

81. Undoubtedly, the existence of some law granting powers of interception of communications to aid the police in their function of investigating and detecting crime may be "necessary in a democratic society ... for the prevention of disorder or crime", within the meaning of paragraph 2 of Article 8 (art. 8-2). The Court accepts, for example, the assertion in the Government's White Paper (at para. 21) that in Great Britain "the increase of crime, and particularly the growth of organised crime, the increasing sophistication of criminals and the ease and speed with which they can move about have made telephone interception an indispensable tool in the investigation and prevention of serious crime". However, the exercise of such powers, because of its inherent secrecy, carries with it a danger of abuse of a kind that is potentially easy in individual cases and could have harmful consequences for democratic society as a whole. This being so, the resultant interference can only be regarded as "necessary in a democratic society" if the particular system of secret surveillance adopted contains adequate guarantees against abuse.

***Klass and Others v Germany*, App No 5029/71, Judgment, European Court of Human Rights**

(6 September 1978)

42. The cardinal issue arising under Article 8 (art. 8) in the present case is whether the interference so found is justified by the terms of paragraph 2 of the Article (art. 8-2). This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions. […]

47. The applicants do not object to the German legislation in that it provides for wide-ranging powers of surveillance; they accept such powers, and the resultant encroachment upon the right guaranteed by Article 8 para. 1 (art. 8-1), as being a necessary means of defence for the protection of the democratic State. The applicants consider, however, that paragraph 2 of Article 8 (art. 8-2) lays down for such powers certain limits which have to be respected in a democratic society in order to ensure that the society does not slide imperceptibly towards totalitarianism. In their view, the contested legislation lacks adequate safeguards against possible abuse.

48. As the Delegates observed, the Court, in its appreciation of the scope of the protection offered by Article 8 (art. 8), cannot but take judicial notice of two important facts. The first consists of the technical advances made in the means of espionage and, correspondingly, of surveillance; the second is the development of terrorism in Europe in recent years. Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.

49. As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion. It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field. Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.

***NG v Direktor na Glavna direktsia 'Natsionalna politsia' pri Ministerstvo na vatreshnite raboti – Sofia* (C-118/22), Judgment, Grand Chamber, Court of Justice of the European Union (30 January 2024)**

40. As stated, in essence, in recital 26 of Directive 2016/680, those requirements are not met where the objective of general interest pursued can reasonably be achieved just as effectively by other means less restrictive of the fundamental rights of the persons concerned (see, by analogy, judgment of 22 June 2021, Latvijas Republikas Saeima (Penalty points), C 439/19, EU:C:2021:504, paragraph 110 and the case-law cited).

51. However, pursuant to Article 16(3) of Directive 2016/680, national law must provide that the data controller is to restrict the processing of those data instead of erasing them where, in accordance with point (a) of that provision, the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained, or where, in accordance with point (b) of that provision, the personal data must be maintained for the purposes of evidence.

54. In that regard, in the first place, it should be noted that the storage, in police records, of data

relating to persons who have been convicted by final judgment may prove necessary for the purposes indicated in the preceding paragraph, even after the conviction in question has been erased from the criminal record and, consequently, the effects which national legislation attaches to that conviction are repealed. Those persons may be involved in criminal offences other than those for which they were convicted or, on the contrary, they may be exonerated through the comparison of the data stored by those authorities with the data collected during the proceedings relating to those other offences.

55. Accordingly, such storage may contribute to the objective of general interest set out in recital 27 of Directive 2016/680, which states that, for the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected (see, to that effect, judgment of 26 January 2023, Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police), C 205/21, EU:C:2023:49, paragraph 98).

59. In that regard, it must be stated, however, that the concept of an 'intentional criminal offence subject to public prosecution' is particularly general and is liable to apply to a large number of criminal offences, irrespective of their nature and gravity (see, to that effect, judgment of 26 January 2023, Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police), C 205/21, EU:C:2023:49, paragraph 129).

60. As the Advocate General also observed, in essence, in points 73 and 74 of his Opinion, persons convicted by final judgment of a criminal offence falling within the scope of that concept do not all present the same degree of risk of being involved in other criminal offences, justifying a uniform period of storage of the data relating to them. Thus, in certain cases, in the light of factors such as the nature and seriousness of the offence committed or the absence of recidivism, the risk represented by the convicted person will not necessarily justify maintaining the data relating to him in the national police records provided for that purpose until his death. In such cases, there will no longer be a necessary connection between the data stored and the objective pursued (see, by analogy, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 205). Accordingly, the storage of such data will not comply with the principle of data minimisation set out in Article 4(1)(c) of Directive 2016/680 and will exceed the period necessary for the purposes for which they are processed, contrary to Article 4(1)(e) of that directive.

61. It must be noted, in that regard, that, admittedly, as the Advocate General stated, in essence, in point 70 of his Opinion, the legal rehabilitation of such a person, resulting in the erasure of his or her conviction from his or her criminal record, such as occurred in the main proceedings, cannot, by itself, render unnecessary the storage of his or her data in the police records, since the purposes of that storage are different from those of the recording of his or her convictions in that criminal record. However, where, as in the present case, under the applicable provisions of national criminal law, such legal rehabilitation is conditional upon the fact that the person concerned has not committed any further intentional criminal offence subject to public prosecution for a certain period of time after the sentence has been served, it may constitute an indication that the person concerned presents a lower risk with regard to the objectives of combating crime or maintaining public order and may therefore be a factor liable to reduce the period for which that storage is necessary.

64. In that context, the Court has held that national legislation which provides for the systematic collection of the biometric and genetic data of any person accused of an intentional offence subject to public prosecution is, in principle, contrary to the requirement of strict necessity laid down in Article 10 of Directive 2016/680 and referred to in paragraph 48 above. Such legislation is liable to lead, in an indiscriminate and generalised manner, to the collection of the biometric and genetic data of most accused persons (see, to that effect, judgment of 26 January 2023, Ministerstvo na

vatreshnite raboti (Recording of biometric and genetic data by the police), C 205/21, EU:C:2023:49, paragraphs 128 and 129).

65. As for the European Court of Human Rights, it has held that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as provided for by the national legislation at issue in the case before that court, failed to strike a fair balance between the competing public and private interests and that, accordingly, the retention of those data constituted a disproportionate interference with the applicants' right to respect for private life and could not be regarded as necessary in a democratic society; that interference thus constituted a violation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 (ECtHR, 4 December 2008, *S. and Marper v. the United Kingdom*, CE:ECHR:2008:1204JUD003056204, §§ 125 and 126).

67. However, the storage of biometric and genetic data can be regarded as meeting the requirement that it is to be allowed only 'where strictly necessary', within the meaning of Article 10 of Directive 2016/680, only if it takes into consideration the nature and seriousness of the offence which led to the final criminal conviction, or other circumstances such as the particular context in which that offence was committed, its possible connection with other ongoing proceedings or the background or profile of the convicted person. Accordingly, where national legislation, such as that at issue in the main proceedings, provides that the biometric and genetic data of data subjects entered in the police records is – in the event that those persons are convicted by final judgment – to be stored until the death of those persons, the scope of that storage is, as stated in paragraphs 59 and 60 above, excessively broad with regard to the purposes for which those data are processed.

69. Consequently, even if the reference, in the national legislation, to the death of the data subject may constitute a 'time limit' for the erasure of stored data, within the meaning of Article 5 of Directive 2016/680, such a time limit can be regarded as 'appropriate' only in specific circumstances which duly justify it. That is clearly not the case where it is applicable generally and indiscriminately to any person convicted by final judgment.

72. In the light of all the foregoing considerations, the answer to the question referred is that Article 4(1)(c) and (e) of Directive 2016/680, read in conjunction with Articles 5 and 10, Article 13(2)(b) and Article 16(2) and (3) thereof, and in the light of Articles 7 and 8 of the Charter, must be interpreted as precluding national legislation which provides for the storage, by police authorities, for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, of personal data, including biometric and genetic data, concerning persons who have been convicted by final judgment of an intentional criminal offence subject to public prosecution, until the death of the data subject, even in the event of his or her legal rehabilitation, without imposing on the data controller the obligation to review periodically whether that storage is still necessary, nor granting that data subject the right to have those data erased, where their storage is no longer necessary for the purposes for which they are processed or, where appropriate, to have the processing of those data restricted.

***V.S. v Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost,* (C-205/21), Judgment, Court of Justice of the European Union (26 January 2023)**

113. Furthermore, as has been observed in paragraphs 46 to 48 of the present judgment, the referring court states that, although those provisions appear to it to require that the competent authorities have a discretion for the purpose of determining whether collection of biometric and genetic data is necessary and that they state adequate reasons for collecting them, the creation of a police record, as provided for by the legislation applicable in the main proceedings, applies mandatorily to all persons accused of intentional offences subject to public prosecution and to the three categories of biometric and genetic data covered by the provision of national law at issue in

the main proceedings, without that legislation requiring the specific necessity to collect all those categories of data to be established.

114. It follows that the fourth question should be understood as seeking to establish, in essence, whether Article 10 of Directive 2016/680, read in conjunction with Article 4(1)(a) to (c) and Article 8(1) and (2) thereof, must be interpreted as precluding national legislation which provides for the systematic collection of biometric and genetic data of any person accused of an intentional offence subject to public prosecution in order for them to be entered in a record, without laying down an obligation on the competent authority to determine and to demonstrate, first, that their collection is necessary for achieving the specific objectives pursued and, second, that those objectives cannot be achieved by collecting only a part of the data concerned.

116. In that regard, in the first place, it should be noted that, as has been stated in paragraphs 62 and 63 of the present judgment, Article 10 of Directive 2016/680 constitutes a specific provision governing processing of the special categories of personal data, including biometric and genetic data. As is clear from the case-law, the purpose of that article is to ensure enhanced protection with regard to that processing, which, because of the particular sensitivity of the data at issue and the context in which they are processed, is liable, as is apparent from recital 37 of the directive, to create significant risks to fundamental rights and freedoms, such as the right to respect for private life and the right to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter (see, by analogy, judgment of 24 September 2019, GC and Others (De-referencing of sensitive data), C-136/17, EU:C:2019:773, paragraph 44).

117. In the second place, as follows from the very terms in which it is set out in Article 10 of Directive 2016/680, the requirement that the processing of such data be allowed 'only where strictly necessary' [('uniquement en cas de nécessité absolue' in the French-language version)] must be interpreted as establishing strengthened conditions for lawful processing of sensitive data, compared with those which follow from Article 4(1)(b) and (c) and Article 8(1) of that directive and refer only to the 'necessity' of data processing that falls generally, within the directive's scope.
118 Thus, first, the use of the adverb 'only' before the words 'where strictly necessary' underlines that the processing of special categories of data, within the meaning of Article 10 of Directive 2016/680, will be capable of being regarded as necessary solely in a limited number of cases. Second, the fact that the necessity for processing of such data is an 'absolute' one [('absolue')] signifies that that necessity is to be assessed with particular rigour.

122. In particular, first, the question whether collection of the biometric and genetic data of accused persons in order for them to be entered in a record is 'strictly necessary', within the meaning of Article 10 of Directive 2016/680, must be determined in the light of the purposes of their collection. In accordance with the purpose limitation principle set out in Article 4(1)(b) of that directive, those purposes must be 'specified, explicit and legitimate'. Second, although the requirement that processing of the biometric and genetic data is to be allowed 'only where strictly necessary' corresponds, as has been observed in paragraphs 117 to 119 of the present judgment, to a requirement for enhanced protection of certain categories of data, it nonetheless constitutes a specific application to the categories of data referred to in Article 10 of the directive of the principle of data minimisation, set out in Article 4(1)(c) of the directive, under which personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

123. Furthermore, in the light of Article 4(1)(a) of Directive 2016/680, the scope of that requirement must also be determined having regard to Article 8(1) thereof, according to which Member States must provide, in particular, for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) of the directive, and to Article 8(2), which requires Member State law regulating processing within the scope of the directive to specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.

125. Furthermore, the requirement that processing of sensitive data be 'strictly necessary' entails particularly strict checking, in that context, as to whether the principle of data minimisation is observed.

126. In that regard, first, it must be borne in mind, as is apparent from recital 26 of Directive 2016/680, that the requirement of necessity is met where the objective pursued by the data processing at issue cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter (see, to that effect, judgment of 1 August 2022, Vyriausioji tarnybinės etikos komisija, C-184/20, EU:C:2022:601, paragraph 85 and the case-law cited). In particular, in the light of the enhanced protection of persons with regard to the processing of sensitive data, the controller in respect of that processing should satisfy itself that that objective cannot be met by having recourse to categories of data other than those listed in Article 10 of Directive 2016/680.

127. Second, having regard to the significant risks posed by the processing of sensitive data to the rights and freedoms of data subjects, in particular in the context of the tasks of the competent authorities for the purposes set out in Article 1(1) of Directive 2016/680, the 'strictly necessary' requirement means that account is to be taken of the specific importance of the objective that such processing is intended to achieve. Such importance may be assessed, inter alia, on the basis of the very nature of the objective pursued – in particular of the fact that the processing serves a specific objective connected with the prevention of criminal offences or threats to public security displaying a certain degree of seriousness, the punishment of such offences or protection against such threats – and in the light of the specific circumstances in which that processing is carried out.

128. In view of the foregoing, it must be held that national legislation which provides for the systematic collection of the biometric and genetic data of any person accused of an intentional offence subject to public prosecution is, in principle, contrary to the requirement laid down in Article 10 of Directive 2016/680 that processing of the special categories of data referred to in that article is to be allowed 'only where strictly necessary'.

131. Thus, first, where there are serious grounds for believing that the person in issue has committed a criminal offence, justifying his or her being accused, a situation which presupposes that sufficient evidence of that person's involvement in the offence has already been gathered, it is possible that the collection both of the biometric data and of the genetic data will not reflect any specific necessity for the purposes of the criminal procedure in progress.

132. Second, the likelihood of the biometric and genetic data of an accused person being strictly necessary in connection with procedures other than the procedure in which that accusation has taken place can be determined only in the light of all the relevant factors, such as, in particular, the nature and gravity of the presumed offence of which he or she is accused, the particular circumstances of that offence, any link between that offence and other procedures in progress, and the criminal record or individual profile of the person in issue.

133. That being so, it is for the referring court to verify whether, in order to ensure the effectiveness of Article 10 of Directive 2016/680, it is possible to interpret the national legislation providing for the enforcement in question in a manner consistent with EU law. In particular, it is for the referring court to verify whether national law enables it to be assessed whether it is 'strictly necessary' to collect both the biometric data and the genetic data of the data subject in order for them to be entered in a record. For that purpose, it should, inter alia, be possible to verify whether the nature and gravity of the offence of which the data subject in the main proceedings is suspected or whether other relevant factors, such as those referred to in paragraph 132 of the present judgment, may constitute circumstances capable of establishing that collection is 'strictly necessary'. Furthermore, it should be checked whether the collection of civil status data, which is also provided for in the context of the

creation of a police record, as the Bulgarian Government confirmed in a written reply to a question asked by the Court, does not in itself enable the objectives pursued to be met.

134. If national law does not guarantee such review of the measure whereby biometric and genetic data are collected, it is for the referring court to ensure that Article 10 of Directive 2016/680 is given full effect by dismissing the police authorities' application requesting it to authorise enforcement of their collection.

135. It follows from all the foregoing that Article 10 of Directive 2016/680, read in conjunction with Article 4(1)(a) to (c) and Article 8(1) and (2) thereof, must be interpreted as precluding national legislation which provides for the systematic collection of biometric and genetic data of any person accused of an intentional offence subject to public prosecution in order for them to be entered in a record, without laying down an obligation on the competent authority to verify whether and demonstrate that, first, their collection is strictly necessary for achieving the specific objectives pursued and, second, those objectives cannot be achieved by measures constituting a less serious interference with the rights and freedoms of the person concerned.

***Spetsializirana prokuratura* (C-350/21), Judgment, Court of Justice of the European Union (17 November 2022) (translated from the original French)**

63. As regards the question whether the national legislation concerned must provide, in a clear and precise manner, that access to stored data is limited to what is strictly necessary in order to achieve the objective pursued by that storage, it follows from the case-law that, in order to satisfy the requirement of proportionality, according to which derogations from, and limitations on, the protection of personal data must be kept within the limits of what is strictly necessary, it is for the competent national authorities to ensure, in each individual case, that both the category or categories of data referred to and the period for which access to them is requested are, having regard to the circumstances of the case, limited to what is strictly necessary for the purposes of the investigation in question (judgment of 2 March 2021 in Case C-746/18 *Prokuratuur (Conditions of access to data relating to electronic communications)* EU: C:2021:152, paragraph 38, and the case-law cited therein).

67. In the light of the foregoing, the answer to the first part of the second question must be that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which does not provide, in a clear and precise manner, that access to stored data is limited to what is strictly necessary to achieve the objective pursued by that storage.

***Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH* (C 793/19 and C 794/19), Judgment, Grand Chamber, Court of Justice of the European Union (20 September 2022)**

92. In the fourth and last place, as regards the European Commission's argument that particularly serious crime could be treated in the same way as a threat to national security, the Court has already held that the objective of protecting national security corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society through the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 61 and the case-law cited).

93. Unlike crime, even particularly serious crime, a threat to national security must be genuine and present, or, at the very least, foreseeable, which presupposes that sufficiently concrete circumstances have arisen to be able to justify a generalised and indiscriminate measure of retention

of traffic and location data for a limited period of time. Such a threat is therefore distinguishable, by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious criminal offences being committed (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 62 and the case-law cited).

94. Thus, crime, even of a particularly serious nature, cannot be treated in the same way as a threat to national security. To treat those situations in the same way would be likely to create an intermediate category between national security and public security for the purpose of applying to the latter the requirements inherent in the former (judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 63). […]

96. In that regard, it must be observed, in the first place, that the effectiveness of criminal proceedings generally depends not on a single means of investigation but on all the means of investigation available to the competent national authorities for those purposes (judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 69).

97. In the second place, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as interpreted by the case-law recalled in paragraph 75 above, allows Member States to adopt, for the purposes of combating serious crime and preventing serious threats to public security, not only measures for targeted retention and expedited retention, but also measures providing for the general and indiscriminate retention, first, of data relating to the civil identity of users of electronic communications systems and, secondly, of IP addresses assigned to the source of a connection (judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 70).

98. In that respect, it is common ground that retention of data relating to the civil identity of users of electronic communications systems may contribute to the fight against serious crime to the extent that those data make it possible to identify persons who have used those means in the context of planning or committing an act constituting serious crime (judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 71).

99. Directive 2002/58 does not preclude, for the purposes of combating crime in general, the generalised retention of data relating to civil identity. In those circumstances, it must be stated that neither the directive nor any other EU law act precludes national legislation, which has the purpose of combating serious crime, pursuant to which the purchase of a means of electronic communication, such as a pre-paid SIM card, is subject to a check of official documents establishing the purchaser's identity and the registration, by the seller, of that information, with the seller being required, should the case arise, to give access to that information to the competent national authorities (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 72).

100. In addition, it should be recalled that the generalised retention of IP addresses of the source of connection constitutes a serious interference in the fundamental rights enshrined in Articles 7 and 8 of the Charter as those IP addresses may allow precise conclusions to be drawn concerning the private life of the user of the means of electronic communication concerned and may be a deterrent to the exercise of freedom of expression guaranteed in Article 11 of the Charter. However, as regards such retention, the Court has held that in order to strike the necessary balance between the rights and interests at issue as required by the case-law referred to in paragraphs 65 to 68 above, it is necessary to take into account, in a case of an offence committed online and, in particular, in cases of the acquisition, dissemination, transmission or making available online of child pornography, within the meaning of Article 2(c) of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ 2011 L 335,

p. 1, and corrigendum OJ 2012 L 18, p. 7), the fact that the IP address might be the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the offence to be identified (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 73).

101. In those circumstances, while it is true that a legislative measure providing for the retention of the IP addresses of all natural persons who own terminal equipment permitting access to the internet would catch persons who at first sight have no connection, within the meaning of the case-law cited in paragraph 70 above, with the objectives pursued, and it is also true, in accordance with what has been stated in paragraph 54 above, that internet users are entitled to expect, under Articles 7 and 8 of the Charter, that their identity will not, in principle, be disclosed, a legislative measure providing for the general and indiscriminate retention of only IP addresses assigned to the source of a connection does not, in principle, appear to be contrary to Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, provided that that possibility is subject to strict compliance with the substantive and procedural conditions which should regulate the use of those data (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 155).

102. In the light of the seriousness of the interference entailed by that retention with the fundamental rights enshrined in Articles 7 and 8 of the Charter, only action to combat serious crime, the prevention of serious threats to public security and the safeguarding of national security are capable of justifying that interference. Moreover, the retention period must not exceed what is strictly necessary in the light of the objective pursued. Finally, a measure of that nature must establish strict conditions and safeguards concerning the use of those data, particularly via tracking, with regard to communications made and activities carried out online by the persons concerned (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 156).

104. In the third place, as regards legislative measures providing for a targeted retention and an expedited retention of traffic and location data, some of the arguments put forward by the Member States against such measures show a narrower understanding of the scope of those measures than that set out in the case-law referred to in paragraph 75 above. While, as is recalled in paragraph 57 above, those retention measures are a derogation within the system established by Directive 2002/58, that directive, read in the light of the fundamental rights enshrined in Articles 7, 8 and 11 and Article 52(1) of the Charter, does not make the possibility of issuing an order requiring a targeted retention subject to the condition either that the places likely to be the location of a serious crime or the persons suspected of being involved in such an act must be known in advance. Likewise, that directive does not require that the order requiring an expedited retention be limited to suspects identified in advance of that order (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 75).

105. As regards, first, targeted retention, the Court has held that Article 15(1) of Directive 2002/58 does not preclude national legislation based on objective evidence which makes it possible to target persons whose traffic and location data are likely to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to combating serious crime or to preventing a serious risk to public security or a risk to national security (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 76 and the case-law cited).

107. Member States thus have, inter alia, the option of imposing retention measures targeting persons who, on the basis of such an identification, are the subject of an investigation or other measures of current surveillance or of a reference in the national criminal record relating to an earlier conviction for serious crimes with a high risk of reoffending. Where that identification is based on objective and non-discriminatory factors, defined in national law, targeted retention in respect of

persons thus identified is justified (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 78).

111. It should also be noted that the geographic areas covered by such a targeted retention measure may and, where appropriate, must be amended in accordance with changes in the circumstances that justified their selection, thus making it possible to react to developments in the fight against serious crime. The Court has held that the duration of those targeted retention measures described in paragraphs 105 to 110 above must not exceed what is strictly necessary in the light of the objective pursued and the circumstances justifying them, without prejudice to the possibility of extending those measures should such retention continue to be necessary (judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 151, and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 82).

123. In that context, it should be recalled that, in paragraph 51 of its judgment of 8 April 2014, Digital Rights Ireland and Others (C-293/12 and C-594/12, EU:C:2014:238), the Court held that while the fight against serious crime is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques, that objective of general interest, however fundamental it may be, does not, in itself, justify that a measure providing for the general and indiscriminate retention of all traffic and location data, such as that established by Directive 2006/24, should be considered to be necessary (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 94).

124. In the same vein, the Court stated, in paragraph 145 of the judgment of 6 October 2020, La Quadrature du Net and Others (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), that even the positive obligations of the Member States which may arise, depending on the circumstances, from Articles 3, 4 and 7 of the Charter and which relate, as pointed out in paragraph 64 above, to the establishment of rules to facilitate effective action to combat criminal offences, cannot have the effect of justifying interference that is as serious as that entailed by national legislation providing for the retention of traffic and location data with the fundamental rights, enshrined in Articles 7 and 8 of the Charter, of practically the entire population, in circumstances where the data of the persons concerned are not liable to disclose a link, at least an indirect one, between those data and the objective pursued (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 95).

***Ligue des droits humains v Conseil des ministres* (C-817/19), Judgment, Grand Chamber, Court of Justice of the European Union (21 June 2022)**

122. To that end, Article 1(2) of the PNR Directive provides that PNR data collected in accordance with that directive may be subject to the processing operations referred to in Article 6(2)(a) to (c) thereof only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Those purposes undoubtedly constitute objectives of general interest of the European Union that are capable of justifying even serious interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter (see, to that effect, judgment of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 42, and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 148 and 149).

123. As to the whether the system established by the PNR Directive is appropriate for the purpose of attaining the objectives pursued, it should be noted that while the possibility of 'false negatives' and the fairly substantial number of 'false positives' resulting, as noted in paragraph 106 above, from automated processing under that directive in 2018 and 2019, are liable to limit the appropriateness of that system, they are not capable, however, of rendering the said system inappropriate for the purpose of contributing to the attainment of the objective of combating terrorist offences and serious crime. As is apparent from the Commission working document referred to in paragraph 106 above, automated processing carried out under the said directive have indeed already made it possible to

identify air passengers presenting a risk in the context of the fight against terrorist offences and serious crime.

140. Accordingly, it must be held that, interpreted in accordance with the considerations set out inter alia in paragraphs 130 to 139 above, Annex I to the PNR Directive is of a sufficiently clear and precise nature overall, thus defining the scope of the interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter.

(2) The purposes for which PNR data may be processed

141. As is apparent from Article 1(2) of the PNR Directive, the PNR data collected in accordance with that directive are to be processed for the purposes of combating 'terrorist offences' and 'serious crime'.

150. In addition, although other offences, also referred to in that Annex II, are less likely, a priori, to be associated with serious crime, it is nevertheless apparent from Article 3(9) of the PNR Directive that those offences may be considered to amount to serious crime only if they are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of the Member State concerned. The requirements flowing from that provision, which relate to the nature and severity of the penalty applicable, are, in principle, such as to limit the application of the system established by that directive to offences that have the requisite level of seriousness to justify the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter stemming from the system established by the said directive.

151. Nonetheless, since Article 3(9) of the PNR Directive refers to the maximum rather than the minimum penalty applicable, it cannot be ruled out that PNR data may be processed for the purposes of combating offences which, although meeting the criterion laid down by that provision relating to the threshold of severity, amount to ordinary crime rather than serious crime, having regard to the particular features of the domestic criminal justice system.

152. It is thus for the Member States to ensure that the application of the system established by the PNR Directive is effectively limited to combating serious crime and that that system does not extend to offences that amount to ordinary crime.

(3) The link between PNR data and the purposes for which those data are processed

153. It is true that, as noted, in essence, by the Advocate General in point 119 of his Opinion, the wording of Article 3(8) and Article 3(9) of the PNR Directive, read in conjunction with Annex II thereto, does not expressly refer to a criterion that is capable of confining the scope of that directive solely to offences that may, by their nature, have an objective link, even if only indirect one, with air travel and, therefore, with the categories of data transferred, processed and retained pursuant to that directive.

154. Nevertheless, as pointed out by the Advocate General in point 121 of his Opinion, certain offences listed in Annex II to the PNR Directive, such as human trafficking, illicit trafficking in narcotic drugs or weapons, facilitation of unauthorised entry and residence and the unlawful seizure of aircraft, are, by their very nature, likely to have a direct link with the carriage of passengers by air. The same is true of certain terrorist offences, such as causing extensive destruction to a transport system or an infrastructure facility or seizure of aircraft, offences under Article 1(1)(d) and (e) of Framework Decision 2002/475, to which Article 3(8) of the PNR Directive refers, or travelling for the purpose of terrorism and organising or otherwise facilitating such travelling, offences under Articles 9 and 10 of Directive 2017/541.

156 In addition, it is important to note that even offences that have no such direct link with the carriage of passengers by air may, depending on the circumstances of the case, have an indirect

link with the carriage of passengers by air. Such is the case, in particular, when air transport is used as a means of preparing such offences or evading criminal prosecution after committing such offences. By contrast, offences having no objective link, not even an indirect one, with the carriage of passengers by air cannot justify the application of the system established by the PNR Directive.

157. In those circumstances, Article 3(8) and (9) of that directive, read in conjunction with Annex II thereto and in the light of the requirements stemming from Articles 7 and 8 as well as Article 52(1) of the Charter, requires Member States, in particular upon individual review by non-automated means as referred to in Article 6(5) of that directive, to ensure that the application of the system established by it be limited to terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.

(4) The air passengers and flights concerned

169. Thus, given recitals 5 to 7, 10 and 22 of the PNR Directive, the Member State must verify that the processing, under that directive, of the PNR data of passengers of intra-EU flights or selected such flights is strictly necessary, having regard to the seriousness of the interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter, in order to ensure the internal security of the European Union or, at least, that of that Member State and, thus, protect the life and safety of persons.

170. As regards, in particular, the threats related to terrorist offences, it is apparent from the Court's case-law that terrorist activities are amongst those capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, particularly, of directly threatening society, the population or the State itself, and that it is of paramount interest for each Member State to prevent and punish those activities to protect the essential functions of the State and the fundamental interests of society in order to safeguard national security. Such threats are distinguishable, by their nature, their particular seriousness and the specific nature of the circumstances of which they are constituted, from the general and permanent risk of serious criminal offences being committed (see, to that effect, judgments of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 135 and 136, and of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraphs 61 and 62).

171. Thus, in a situation where it is established, on the basis of the assessment carried out by a Member State, that there are sufficiently solid grounds for considering that the latter is confronted with a terrorist threat which is shown to be genuine and present or foreseeable, the fact that that Member State makes provision for the application of the PNR Directive, pursuant to Article 2(1) of that directive, to all intra-EU flights from or to the said Member State, for a limited period of time, does not appear to go beyond what is strictly necessary. The existence of that threat is, in itself, capable of establishing a connection between, on the one hand, the transfer and processing of the data concerned and, on the other, the fight against terrorism (see, by analogy, judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 137).

173. By contrast, in the absence of a genuine and present or foreseeable terrorist threat with which the Member State concerned is confronted, the indiscriminate application by that Member State of the system established by the PNR Directive not only to extra-EU flights but also to all intra-EU flights would not be considered to be limited to what is strictly necessary.

175. It follows from the foregoing that the interpretation, thus followed, of Article 2 and Article 3(4) of the PNR Directive, in the light of Articles 7 and 8 as well as Article 52(1) of the Charter, is capable of ensuring that those provisions are within the limits of what is strictly necessary.

248. By its Question 8, the referring court asks, in essence, whether Article 12 of the PNR Directive, read in conjunction with Articles 7 and 8 as well as Article 52(1) of the Charter, must be interpreted as precluding national legislation which provides for a general retention period of five years for PNR data, without drawing any distinction based on whether or not the passengers concerned present a risk that relates to terrorist offences or serious crime.

258. The continued storage of the PNR data of all air passengers after the initial period of six months is not therefore limited to what is strictly necessary (see, by analogy Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 206).

259. However, in so far as, in specific cases, objective material, such as the PNR data of passengers which gave rise to a verified positive match, is identified from which it may be inferred that certain passengers may present a risk that relates to terrorist offences or serious crime, it seems permissible to store their PNR data beyond that initial period (see, by analogy, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 207 and the case-law cited).

260. Identification of that objective material is capable of establishing a connection with the objectives pursued by processing under the PNR Directive, with the result that the retention of the PNR data of those passengers is justified during the maximum period permitted by the said directive, namely during five years.

***G.D. v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, and Attorney General*, (C-140/20), Judgment, Grand Chamber, Court of Justice of the European Union (5 April 2022)**

41. As regards the objectives that are capable of justifying a limitation of the rights and obligations laid down, in particular, in Articles 5, 6 and 9 of Directive 2002/58, the Court has previously held that the list of objectives set out in the first sentence of Article 15(1) of that directive is exhaustive, as a result of which a legislative measure adopted under that provision must correspond, genuinely and strictly, to one of those objectives (judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 112 and the case-law cited).

52. In that regard, it should be borne in mind that the protection of the fundamental right to privacy requires, according to the settled case-law of the Court, that derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 130 and the case-law cited).

53. More specifically, it follows from the Court's case-law that the question whether the Member States may justify a limitation on the rights and obligations laid down, inter alia, in Articles 5, 6 and 9 of Directive 2002/58 must be assessed by measuring the seriousness of the interference entailed by such a limitation and by verifying that the importance of the public interest objective pursued by that limitation is proportionate to that seriousness (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 131 and the case-law cited).

61. However, the Court has already held that the objective of protecting national security corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society through the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities (see, to that effect, judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 135).

62. It should also be observed that, unlike crime, even particularly serious crime, a threat to national security must be genuine and present, or, at the very least, foreseeable, which presupposes that sufficiently concrete circumstances have arisen to be able to justify a generalised and indiscriminate measure of retention of traffic and location data for a limited period of time. Such a threat is therefore distinguishable, by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious criminal offences being committed (see, to that effect, judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 136 and 137).

63. Thus, criminal behaviour, even of a particularly serious nature, cannot be treated in the same way as a threat to national security. […]

65. As regards the objective of combating serious crime, the Court held that national legislation providing, for that purpose, for the general and indiscriminate retention of traffic and location data exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society. In view of the sensitive nature of the information that traffic and location data may provide, the confidentiality of those data is essential for the right to respect for private life. […]

69. […] it must be observed, in the first place, that the effectiveness of criminal proceedings generally depends not on a single means of investigation but on all the means of investigation available to the competent national authorities for those purposes.

70. In the second place, it must be noted that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as interpreted by the case-law recalled in paragraph 67 of this judgment, allows Member States to adopt, for the purposes of combating serious crime and preventing serious threats to public security, not only measures for targeted retention and expedited retention, but also measures providing for the general and indiscriminate retention, first, of data relating to the civil identity of users of electronic communications systems and, second, of IP addresses assigned to the source of a connection.

71. In that respect, it is common ground that retention of data relating to the civil identity of users of electronic communications systems may contribute to the fight against serious crime to the extent that those data make it possible to identify persons who have used those means in the context of planning or committing an act constituting serious crime.

72. As is clear from the case-law summarised in paragraph 67 of this judgment, Directive 2002/58 does not preclude, for the purposes of combating crime in general, the general retention of data relating to civil identity. In those circumstances, it must be stated that neither the directive nor any other EU law act precludes national legislation, which has the purpose of combating serious crime, pursuant to which the purchase of a means of electronic communication, such as a pre-paid SIM card, is subject to a check of official documents establishing the purchaser's identity and the registration, by the seller, of that information, with the seller being required, should the case arise, to give access to that information to the competent national authorities.

73. In addition, it should be recalled that the generalised retention of IP addresses of the source of connection constitutes a serious interference in the fundamental rights enshrined in Articles 7 and 8 of the Charter as those IP addresses may allow precise conclusions to be drawn concerning the private life of the user of the means of electronic communication concerned and may be a deterrent to the exercise of freedom of expression guaranteed in Article 11 of the Charter. However, as regards such retention, the Court has held that in order to strike the necessary balance between the rights and interests at issue as required by the case-law referred to in paragraphs 50 to 53 of this judgment, it is necessary to take into account, in a case of an offence committed online and, in particular, in cases of the acquisition, dissemination, transmission or making available online of child

pornography, within the meaning of Article 2(c) of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ 2011 L 335, p. 1), the fact that the IP address might be the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the offence to be identified (see, to that effect, judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 153 and 154).

74. Hence, the Court held that such general and indiscriminate retention solely of IP addresses assigned to the source of a connection does not, in principle, appear to be contrary to Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 of the Charter, provided that that possibility is subject to strict compliance with the substantive and procedural conditions which should regulate the use of those data, as referred to in paragraphs 155 and 156 of the judgment of 6 October 2020, La Quadrature du Net and Others (C-511/18, C-512/18 and C-520/18, EU:C:2020:791).

75. In the third place, as regards legislative measures providing for a targeted retention and an expedited retention of traffic and location data, the indications provided in the order for reference show a narrower understanding of the scope of those measures than that upheld in the case-law recalled in paragraph 67 of this judgment. While, as is recalled in paragraph 40 of this judgment, those retention measures are a derogation within the system established by Directive 2002/58, that directive, read in the light of the fundamental rights enshrined in Articles 7, 8 and 11 and Article 52(1) of the Charter, does not make the possibility of issuing an order requiring a targeted retention subject to the condition either that the places likely to be the location of a serious crime or the persons suspected of being involved in such an act must be known in advance. Likewise, that directive does not require that the order requiring an expedited retention be limited to suspects identified in advance of that order.

76. As regards, first, targeted retention, the Court held that Article 15(1) of Directive 2002/58 does not preclude national legislation based on objective evidence which makes it possible to target persons whose traffic and location data are likely to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to combating serious crime or to preventing a serious risk to public security or a risk to national security (judgments of 21 December 2016, Tele2 Sverige and Watson and Others, C-203/15 and C-698/15, EU:C:2016:970, paragraph 111, and of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 148).

78. Member States thus have, inter alia, the option of imposing retention measures targeting persons who, on the basis of an identification, are the subject of an investigation or other measures of current surveillance or of a reference in the national criminal record relating to an earlier conviction for serious crimes with a high risk of reoffending. Where that identification is based on objective and non-discriminatory factors, defined in national law, targeted retention in respect of persons thus identified is justified.

80. It should be borne in mind that, according to that case-law, the competent national authorities may adopt, for areas referred to in the preceding paragraph, a targeted measure of retention using a geographic criterion, such as, inter alia, the average crime rate in a geographical area, without that authority necessarily having specific indications as to the preparation or commission, in the areas concerned, of acts of serious crime. Since a targeted retention using that criterion is likely to concern, depending on the serious criminal offences in question and the situation specific to the respective Member States, both the areas marked by a high incidence of serious crime and areas particularly vulnerable to the commission of those acts, it is, in principle, not likely moreover to give rise to discrimination, as the criterion drawn from the average rate of serious crime is entirely unconnected with any potentially discriminatory factors.

81. In addition and above all, a targeted measure of retention covering places or infrastructures which regularly receive a very high volume of visitors, or strategic places, such as airports, stations, maritime ports or tollbooth areas, allows the competent authorities to collect traffic data and, in particular, location data of all persons using, at a specific time, a means of electronic communication in one of those places. Thus, such a targeted retention measure may allow those authorities to obtain, through access to the retained data, information as to the presence of those persons in the places or geographical areas covered by that measure as well as their movements between or within those areas and to draw, for the purposes of combating serious crime, conclusions as to their presence and activity in those places or geographical areas at a specific time during the period of retention.

82. It should also be noted that the geographic areas covered by such a targeted retention measure may and, where appropriate, must be amended in accordance with changes in the circumstances that justified their selection, thus making it possible to react to developments in the fight against serious crime. The Court has held that the duration of those targeted retention measures described in paragraphs 76 to 81 of this judgment must not exceed what is strictly necessary in the light of the objective pursued and the circumstances justifying them, without prejudice to the possibility of extending those measures should such retention continue to be necessary (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 151).

94. In that context, it should be recalled that, in paragraph 51 of its judgment of 8 April 2014, Digital Rights Ireland and Others (C-293/12 and C-594/12, EU:C:2014:238), the Court held that while the fight against serious crime is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques, that objective of general interest, however fundamental it may be, does not, in itself, justify that a measure providing for the general and indiscriminate retention of all traffic and location data, such as that established by Directive 2006/24, should be considered to be necessary.

95. In the same vein, the Court stated, in paragraph 145 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), that even the positive obligations of the Member States which may arise, depending on the circumstances, from Articles 3, 4 and 7 of the Charter and which relate, as pointed out in paragraph 49 of this judgment, to the establishment of rules to facilitate effective action to combat criminal offences, cannot have the effect of justifying interference that is as serious as that entailed by legislation providing for the retention of traffic and location data with the fundamental rights, enshrined in Articles 7 and 8 of the Charter, of practically the entire population, in circumstances where the data of the persons concerned are not liable to disclose a link, at least an indirect one, between those data and the objective pursued.

105. Accordingly, since general access to all retained data, regardless of whether there is any, at least indirect, link with the intended purpose, cannot be regarded as being limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data in question. In that regard, such access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that those data might, in a specific case, make an effective contribution to combating such activities (judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 50 and the case-law cited).

Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary

***of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service* (C-623/17), Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2020)**

51. […] section 94 of the 1984 Act permits the Secretary of State to require providers of electronic communications services, by way of directions, if he considers it necessary in the interests of national security or relations with a foreign government, to forward bulk communications data to the security and intelligence agencies. That data includes traffic data and location data, as well as information relating to the services used, pursuant to section 21(4) and (6) of the RIPA. That provision covers, inter alia, the data necessary to (i) identify the source and destination of a communication, (ii) determine the date, time, length and type of communication, (iii) identify the hardware used, and (iv) locate the terminal equipment and the communications. That data includes, inter alia, the name and address of the user, the telephone number of the person making the call and the number called by that person, the IP addresses of the source and addressee of the communication and the addresses of the websites visited.

52. Such a disclosure of data by transmission concerns all users of means of electronic communication, without its being specified whether that transmission must take place in real-time or subsequently. Once transmitted, that data is, according to the information set out in the request for a preliminary ruling, retained by the security and intelligence agencies and remains available to those agencies for the purposes of their activities, as with the other databases maintained by those agencies. In particular, the data thus acquired, which is subject to bulk automated processing and analysis, may be cross-checked with other databases containing different categories of bulk personal data or be disclosed outside those agencies and to third countries. Lastly, those operations do not require prior authorisation from a court or independent administrative authority and do not involve notifying the persons concerned in any way.

55. Thus, Article 5(1) of that directive enshrines the principle of confidentiality of both electronic communications and the related traffic data and requires, inter alia, that, in principle, persons other than users be prohibited from storing, without those users' consent, those communications and that data. Having regard to the general nature of its wording, that provision necessarily covers any operation enabling third parties to become aware of communications and data relating thereto for purposes other than the conveyance of a communication.

58. However, Article 15(1) of Directive 2002/58 enables the Member States to introduce an exception to the obligation of principle, laid down in Article 5(1) of that directive, to ensure the confidentiality of personal data, and to the corresponding obligations, referred to, inter alia, in Articles 6 and 9 of that directive, where this constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence and public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. To that end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on one of those grounds.

67. In that regard, it should be borne in mind that the protection of the fundamental right to privacy requires, according to the settled case-law of the Court, that derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue.

75. […] Subject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives […].

77. In particular, as regards an authority's access to personal data, legislation cannot confine itself to requiring that authorities' access to the data be consistent with the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use […].

81. It follows that national legislation requiring providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter.

82. In the light of all the foregoing considerations, the answer to the second question is that Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation enabling a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security.

***Digital Rights Ireland Ltd v Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others* (C-594/12), Joined Cases, Judgment, Grand Chamber, Court of Justice of the European Union (8 April 2014)**

42. It is apparent from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest. The same is true of the fight against serious crime in order to ensure public security. Furthermore, it should be noted, in this respect, that Article 6 of the Charter lays down the right of any person not only to liberty, but also to security.

43. In this respect, it is apparent from recital 7 in the preamble to Directive 2006/24 that, because of the significant growth in the possibilities afforded by electronic communications, the Justice and Home Affairs Council of 19 December 2002 concluded that data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime.

44. It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest. […]

51. As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.

52. So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet OEA/Ser.L/V/II. CIDH/RELE/INF.11/13 (31 December 2013)

157. […] limitations to the rights guaranteed by the American Convention must pursue compelling objectives agreed to by the States through their signature of international human rights law

instruments. In the case of State surveillance activities—on the Internet or in any other sphere—reasons of national security and the fight against crime or organized crime tend to be invoked. The Office of the Special Rapporteur has maintained that when national security is invoked as a reason for monitoring personal data and correspondence, in order to prevent discretionary interpretations, the law must clearly specify the criteria to be applied in determining the cases in which these types of limitations are legitimate, and it must be careful to define that concept precisely. In particular, the Office of the Special Rapporteur has asserted that the concept of national security cannot be interpreted haphazardly and must be defined from a democratic perspective.

158. The inter-American system for the protection of human rights has ruled, for example, on inadmissible interpretations of the concept of national security. In the case of *Molina-Theissen v. Guatemala*, the Inter-American Court of Human Rights held that the so-called "national security doctrine" makes it possible to characterize a person as 'subversive' or as an 'internal enemy,' for the sole fact that they genuinely or allegedly supported the fight to change the established order. Similarly, in the case of *Goiburu et al. v. Paraguay* the Court found that "[m]ost of the Southern Cone's dictatorial governments assumed power or were in power during the 1970s [...]. The ideological basis of all these regimes was the 'National Security Doctrine,' which regarded leftist movements and other groups as 'common enemies'." Even today, it has been reported that national security reasons tend to be invoked to place human rights defenders, journalists, members of the media, and activists under surveillance, or to justify excessive secrecy in the decision-making processes and investigations tied to surveillance issues. Clearly, this kind of interpretation of the "national security" objective cannot be the basis for the establishment of surveillance programs of any kind, including, naturally, online communications surveillance programs.

159. […] in order for an online communications surveillance program to be appropriate, States must demonstrate that the limitations to the rights to privacy and freedom of expression arising from those programs are strictly necessary in a democratic society to accomplish the objectives they pursue.

160. The opinion of strict necessity with respect to communications surveillance assumes that it is insufficient for the measure to be "useful," "reasonable," or "opportune." In order for the restriction to be legitimate, the true and compelling need to impose the limitation must be clearly established; that is, said legitimate and compelling aim cannot be reasonably accomplished by any other means less restrictive of human rights.

D. THE PRINCIPLE OF PROPORTIONALITY

The review of pronouncements by different human rights monitoring mechanisms shows that there are significant overlaps in references to the principles of legality, necessity and proportionality. Whether an appraisal is made within the test of necessity or proportionality will also often depend on the particular approach adopted by the court in question. This is particularly the case for the principles of necessity and proportionality, as well as whether the aim pursued is an element in the assessment of necessity, or of legality. It may therefore be pertinent to also consult other sub-chapters. Reference to the principle of legality within the broader framework of principles governing surveillance can be found in the introductory sub-chapter A.

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

25. Moreover, the impact of most encryption restrictions on the right to privacy and associated rights are disproportionate, often affecting not only the targeted individuals but the general population. Outright bans by Governments, or the criminalization of encryption in particular, cannot be justified as they would prevent all users within their jurisdictions from having a secure way to communicate. Key escrow systems have significant vulnerabilities, since they depend on the integrity of the storage facility and expose stored keys to cyberattacks. Moreover, mandated back doors in encryption tools create liabilities that go far beyond their usefulness with regard to specific users identified as crime suspects or security threats. They jeopardize the privacy and security of all users and expose them to unlawful interference, not only by States, but also by non-State actors, including criminal networks. Licensing and registration requirements have similar disproportionate effects as they require that encryption software contain exploitable weaknesses. Such adverse effects are not necessarily limited to the jurisdiction imposing the restriction; rather it is likely that back doors, once established in the jurisdiction of one State, will become part of the software used in other parts of the world.

52. General monitoring of people in public spaces is almost invariably disproportionate. Surveillance measures in public spaces should be targeted and should address a concrete legitimate aim, such as averting a specific threat to public safety or security that is significant enough to outweigh their adverse human rights impacts. Such measures need to be limited, focused on specific locations and times, for instance, when evidence indicates that a crime is likely to occur or that threats to public safety and security may emerge. No less privacy- invasive alternative should be available. It is essential to impose strict limitations on the duration of storage of captured data and the associated purposes for which such data is to be used. Remote biometric surveillance systems, in particular, raise serious concerns with regard to their proportionality, given their highly intrusive nature and broad impact on large numbers of people. […]

Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, UN Doc A/75/590 (10 November 2020)

27. In Austria, Belgium, Denmark, Germany, Norway and the United Kingdom of Great Britain and Northern Ireland, laws allow for the seizure of mobile phones from asylum or migration applicants, from which data are then extracted and used as part of asylum procedures. These practices constitute a serious, disproportionate interference with migrants' and refugees' right to privacy, on the basis of immigration status and, in effect, national origin. Furthermore, the

presumption that data obtained from digital devices necessarily leads to reliable evidence is flawed. […] Some of these activities are undertaken directly by government officials themselves, but in some instances, governments call on companies to provide them with the tools and/or know-how to undertake this surveillance.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/29/32 (22 May 2015)

35. Necessity also implies an assessment of the proportionality of the measures limiting the use of and access to security online. A proportionality assessment should ensure that the restriction is "the least intrusive instrument amongst those which might achieve the desired result". The limitation must target a specific objective and not unduly intrude upon other rights of targeted persons, and the interference with third parties' rights must be limited and justified in the light of the interest supported by the intrusion. The restriction must also be "proportionate to the interest to be protected". A high risk of damage to a critical, legitimate State interest may justify limited intrusions on the freedom of expression. Conversely, where a restriction has a broad impact on individuals who pose no threat to a legitimate government interest, the State's burden to justify the restriction will be very high. Moreover, a proportionality analysis must take into account the strong possibility that encroachments on encryption and anonymity will be exploited by the same criminal and terrorist networks that the limitations aim to deter. In any case, "a detailed and evidence-based public justification" is critical to enable transparent public debate over restrictions that implicate and possibly undermine freedom of expression. [...]

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014)

18. Assuming therefore that there remains a legal right to respect for the privacy of digital communications (and this cannot be disputed (see General Assembly resolution 68/167)), the adoption of mass surveillance technology undoubtedly impinges on the very essence of that right. It is potentially inconsistent with the core principle that States should adopt the least intrusive means available when entrenching on protected human rights; it excludes any individualized proportionality assessment; and it is hedged around by secrecy claims that make any other form of proportionality analysis extremely difficult.

51. It is incumbent upon States to demonstrate that any interference with the right to privacy under article 17 of the Covenant is a necessary means to achieving a legitimate aim. This requires that there must be a rational connection between the means employed and the aim sought to be achieved. It also requires that the measure chosen be "the least intrusive instrument among those which might achieve the desired result". The related principle of proportionality involves balancing the extent of the intrusion into Internet privacy rights against the specific benefit accruing to investigations undertaken by a public authority in the public interest. However, there are limits to the extent of permissible interference with a Covenant right. As the Human Rights Committee has emphasized, "in no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right". In the context of covert surveillance, the Committee has therefore stressed that any decision to allow interference with communications must be taken by the authority designated by law "on a case- by-case basis". The proportionality of any interference with the right to privacy should therefore be judged on the particular circumstances of the individual case.

52. The technical ability to run vast data collection and analysis programmes undoubtedly offers an additional means by which to pursue counter-terrorism and law enforcement investigations. But an assessment of the proportionality of these programmes must also take account of the collateral damage to collective privacy rights. Mass data collection programmes appear to offend

against the requirement that intelligence agencies must select the measure that is least intrusive on human rights (unless relevant States are in a position to demonstrate that nothing less than blanket access to all Internet-based communication is sufficient to protect against the threat of terrorism and other serious crime). Since there is no opportunity for an individualized proportionality assessment to be undertaken prior to these measures being employed, such programmes also appear to undermine the very essence of the right to privacy. They exclude altogether the "case-by-case" analysis that the Human Rights Committee has regarded as essential, and they may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. The Special Rapporteur, accordingly, concludes that such programmes can be compatible with article 17 of the Covenant only if relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people in any part of the world. [...]

***Digital Rights Ireland Ltd v Minister of Communications, Marine and Natural Resources et al.* (C-293/12); *Kärntner Landesregierung and oth*ers (C-594/12), Joined Cases, Judgment, Grand Chamber, Court of Justice of the European Union (8 April 2014)**

46. In that regard, according to the settled case-law of the Court, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives.

47. With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference.

48. In the present case, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, UN Doc A/HRC/23/40 (17 April 2013)

83. Legal frameworks must ensure that communications surveillances measures: […] (c) adhere to the principle of proportionality, and are not employed when less invasive techniques are available or have not yet been exhausted.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc A/HRC/13/37 (28 December 2009)

49. [Right to privacy protections] require States to have exhausted less-intrusive techniques before resorting to others […] States must incorporate this principle into existing and future policies as they present how their policies are necessary, and in turn proportionate"

UN Human Rights Committee, General Comment No 16: Article 17 (Right to Privacy), UN Doc HRI/GEN/1/Rev.1 (8 April 1988)

The expression "arbitrary interference" is also relevant to the protection of the right provided for in

article 17. In the Committee's view the expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.

***Toonen v Australia*, Comm No 488/1992, Human Rights Committee, UN Doc CCPR/C/50/D/488/1992 (31 March 1994)**

8.3 [...] any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case.

***N.F. and Others v Russia*, Apps Nos 3537/15 and 8 others, Judgment, European Court of Human Rights (12 September 2023)**

46. The Court has considered a series of cases relating to the retention and processing of personal data of individuals convicted of criminal offences and of individuals who had been suspected of committing criminal offences, but who had ultimately been discharged. In its assessment of the proportionality of the interference in those cases the Court has had regard to the following elements: the nature and gravity of the offences in question; the level of the actual interference with the right to respect for private life; the scope and application of the data storage system; the data retention period; the possibility of review; safeguards against abuse; and guarantees aimed at regulating access by third parties and protecting data integrity and confidentiality (see, for instance, *S. and Marper*, cited above, §§ 118-24; *Gardel*, cited above, §§ 65-70; and *Gaughran v. the United Kingdom*, no. 45245/15, §§ 94 and 96, 13 February 2020, with further references).

47. A margin of appreciation must be left to the relevant national authorities in such an assessment. The breadth of this margin varies and depends on a number of factors, including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference. The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights. Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State will be restricted. Where, however, there is no consensus within the member States of the Council of Europe – either as to the relative importance of the interest at stake or as to how best to protect it – the margin will be wider (see *S. and Marper*, cited above, §102).

49. Regarding the scope and application of the data storage system, the Court observes that the recording system in place covers not only criminal convictions but also situations where an individual has been subjected to criminal prosecution and the criminal proceedings were subsequently discontinued on "non-rehabilitative grounds". Thus, a significant amount of data is collected and stored in databases once an individual is subjected to criminal prosecution. Moreover, data relating to criminal convictions are collected and stored, irrespective of the nature and gravity of the offence committed. It was not contested by the Government that both the collection and initial storage of those data are intended to be automatic, and that their further storage is also automatic. Therefore, the scope and application of this system are extensive.

50. The Court further observes that the procedure and the time-limits for the storage and processing of data are governed by Ministry orders no. 612 of 9 July 2007 and no. 89 of 12 February 2014, which are classified confidential, have never been published in any official publication and are not accessible to the public (see paragraphs 15 and 25 above). It was deemed by the domestic courts (which referred to these orders) that such data should be stored until the subject in question reached the age of eighty years. Under the Personal Data Act and the Police Act, personal data must be destroyed once the aims pursued by their processing have been achieved or in the event that it is no longer necessary to pursue those aims. However, since the relevant Ministry orders are classified as confidential, the discretion afforded to the Ministry in the exercise of this power is not

counterbalanced by sufficient guarantees against abuse, and the possibility of any review would appear to be almost hypothetical (see, mutatis mutandis, *Gaughran*, cited above, § 94; also contrast with *N. v. Germany*, cited above, §§ 85-88). The available legal framework failed to make any distinction based on the purpose of the processing of the data, such as providing information in the context of employment, and, as a result, at no point the proportionality and the existence of relevant and sufficient reasons for the interference with the applicants' right to respect for their private life were assessed.

52. Lastly, the Court acknowledges that the level of interference with the applicants' right to a private life may differ according to whether the applicant was convicted or whether the charges were dropped.

53. The continued processing of data is particularly intrusive for applicants who have not been convicted of any criminal offences. The Court has already expressed its concerns about the risk of stigmatisation, which stems from the fact that such persons, who are entitled to presumption of innocence, have in the past been treated in the same way as convicted persons (see *S. and Marper*, cited above, § 122).

54. In so far as convicted persons are concerned, the level of interference with their private life will also be intrusive after their convictions have become spent or are lifted by a court; this is particularly so in respect of their social reintegration (see Recommendation No. R (84) 10 of the Committee of Ministers on the criminal record and rehabilitation of convicted persons, "Relevant Council of Europe Instruments" above, paragraph 27).

55. In conclusion, the Court finds that the processing of the applicants' data relating to criminal convictions which have become spent or which have been lifted by a court and of data relating to criminal proceedings which have been discontinued on "non-rehabilitative grounds" failed to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, such processing constituted a disproportionate interference with the applicants' right to respect for their private life and cannot be regarded as "necessary in a democratic society".

***Catt v The United Kingdom*, App No 43514/15, Judgment, European Court of Human Rights (24 January 2019)**

111. The Court recalls that in Article 8 cases it has generally understood the margin of appreciation to mean that, where the independent and impartial domestic courts have carefully examined the facts, applying the relevant human rights standards consistently with the Convention and its case-law, and adequately balanced the applicant's personal interests against the more general public interest in the case, it is not for it to substitute its own assessment of the merits (including, in particular, its own assessment of the factual details of proportionality) for that of the competent national authorities, unless there are shown to be compelling reasons for doing so.

***Ivashchenko v Russia*, App No 61064/10, Judgment, European Court of Human Rights (13 February 2018)**

76. As regards specifically searches and seizures or similar measures (essentially in the context of obtaining physical evidence of certain offences), it is pertinent to assess whether the reasons adduced to justify such measures were relevant and sufficient and whether the proportionality principle has been adhered to. […]

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet OEA/Ser.L/V/II. CIDH/RELE/INF.11/13 (31 December 2013)

161. In any case, as has been mentioned, in order to define if a measure is proportioned, its impact on the capacity of the Internet to guarantee and promote freedom of expression should be evaluated.

162. Given the importance of the exercise of these rights in a democratic system, the law must authorize access to personal data and communications only under the most exceptional circumstances defined in the law. When fairly open-ended grounds such as national security are invoked as the reason to monitor personal data and correspondence, the law must clearly specify the criteria to be applied in determining those cases in which such limitations are legitimate. Their application should be authorized solely when there is a definite risk to the protected interests, and when that harm is greater than society's general interest in maintaining the rights to privacy and the free expression of thought and the circulation of information.

***NG v Direktor na Glavna direktsia 'Natsionalna politsia' pri Ministerstvo na vatreshnite raboti – Sofia* (C-118/22), Judgment, Grand Chamber, Court of Justice of the European Union (30 January 2024)**

41 In the second place, first of all, under Article 4(1)(c) of that directive, Member States are to provide for personal data to be adequate, relevant and not excessive in relation to the purposes for which they are processed. That provision thus requires the Member States to observe the principle of 'data minimisation', which gives expression to the principle of proportionality (see, to that effect, judgment of 22 June 2021, Latvijas Republikas Saeima (Penalty points), C 439/19, EU:C:2021:504, paragraph 98 and the case-law cited).

62 In the fifth place, the principle of proportionality, set out in Article 52(1) of the Charter, entails, in particular, a balancing of the importance of the objective pursued and the seriousness of the limitation placed on the exercise of the fundamental rights in question (see, to that effect, judgment of 22 November 2022, Luxembourg Business Registers, C 37/20 and C 601/20, EU:C:2022:912, paragraph 66).

63 In the present case, as noted in paragraph 35 above, the storage of personal data in the police register at issue includes biometric and genetic data. It must therefore be pointed out that, having regard to the significant risks posed by the processing of such sensitive data to the rights and freedoms of data subjects, in particular in the context of the tasks of the competent authorities for the purposes set out in Article 1(1) of Directive 2016/680, the specific importance of the objective pursued must be assessed in the light of a number of relevant factors. Such factors include, inter alia, the fact that the processing serves a specific objective connected with the prevention of criminal offences or threats to public security displaying a certain degree of seriousness, the punishment of such offences or protection against such threats, and the specific circumstances in which that processing is carried out (judgment of 26 January 2023, Ministerstvo na v atreshnite raboti (Recording of biometric and genetic data by the police), C 205/21, EU:C:2023:49, paragraph 127).

***Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH* (C 793/19 and C 794/19), Judgment, Grand Chamber, Court of Justice of the European Union (20 September 2022)**

58. As regards the objectives that are capable of justifying a limitation of the rights and obligations laid down, in particular, in Articles 5, 6 and 9 of Directive 2002/58, the Court has previously held that the list of objectives set out in the first sentence of Article 15(1) of that directive is exhaustive, as a result of which a legislative measure adopted under that provision must correspond, genuinely and strictly, to one of those objectives (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 41 and the case-law cited).

59. Furthermore, it is clear from the third sentence in Article 15(1) of Directive 2002/58 that measures taken by the Member States must comply with the general principles of EU law, which include the

principle of proportionality, and ensure respect for the fundamental rights guaranteed by the Charter. In that regard, the Court has previously held that the obligation imposed on providers of electronic communications services by a Member State by way of national legislation to retain traffic data for the purpose of making them available, if necessary, to the competent national authorities raises issues relating to compatibility not only with Articles 7 and 8 of the Charter, but also with Article 11 of the Charter, relating to the freedom of expression, which constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the European Union is founded (see, to that effect, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraphs 42 and 43 and the case-law cited).

64. Thus as regards, in particular, effective action to combat criminal offences committed against, inter alia, minors and other vulnerable persons, it should be borne in mind that positive obligations of the public authorities may result from Article 7 of the Charter, requiring them to adopt legal measures to protect private and family life. Such obligations may also arise from Article 7, concerning the protection of an individual's home and communications, and Articles 3 and 4, as regards the protection of an individual's physical and mental integrity and the prohibition of torture and inhuman and degrading treatment (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 49 and the case-law cited).

65. In view of those different positive obligations, it is therefore necessary to strike a balance between the various interests and rights at issue and to establish a legal framework which enables such a balance to be struck (see, to that effect, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 50 and the case-law cited).

66. In that context, it is clear from the wording itself of the first sentence of Article 15(1) of Directive 2002/58 that the Member States may adopt a measure derogating from the principle of confidentiality referred to in paragraph 52 above where such a measure is 'necessary, appropriate and proportionate within a democratic society', and recital 11 of the directive specifies, in that respect, that a measure of that nature must be 'strictly' proportionate to the intended purpose.

67. In that regard, it should be borne in mind that the protection of the fundamental right to privacy requires, according to the settled case-law of the Court, that derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 52 and the case-law cited).

68. More specifically, it follows from the Court's case-law that the question whether the Member States may justify a limitation on the rights and obligations laid down, inter alia, in Articles 5, 6 and 9 of Directive 2002/58 must be assessed by measuring the seriousness of the interference entailed by such a limitation and by verifying that the importance of the public interest objective pursued by that limitation is proportionate to that seriousness (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 53 and the case-law cited).

69. In order to satisfy the requirement of proportionality, the national legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that those data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data are subjected to automated processing, in particular where there is a significant risk of unlawful access to those data. Those considerations

apply especially where the protection of the particular category of personal data that are sensitive data is at stake (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 54 and the case-law cited).

70. Thus, national legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the data to be retained and the objective pursued (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 55 and the case-law cited).

71. As regards the public interest objectives that may justify a measure taken pursuant to Article 15(1) of Directive 2002/58, it is clear from the Court's case-law, in particular the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), that, in accordance with the principle of proportionality, there is a hierarchy amongst those objectives according to their respective importance and that the importance of the objective pursued by such a measure must be proportionate to the seriousness of the interference that it entails (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 56).

72. Thus, as regards safeguarding national security, the importance of which exceeds that of the other objectives referred to in Article 15(1) of Directive 2002/58, the Court held that that provision, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, does not preclude legislative measures that allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 58 and the case-law cited).

73. As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, the Court held that, in accordance with the principle of proportionality, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data. Accordingly, only non-serious interference with those fundamental rights may be justified by the objective of preventing, detecting and prosecuting criminal offences in general (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 59 and the case-law cited).

74. As regards the objective of combating serious crime, the Court held that national legislation providing, for that purpose, for the general and indiscriminate retention of traffic and location data exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society. In view of the sensitive nature of the information that traffic and location data may provide, the confidentiality of those data is essential for the right to privacy. Thus, and also taking into account, first, the dissuasive effect on the exercise of the fundamental rights enshrined in Articles 7 and 11 of the Charter, referred to in paragraph 62 above, which is liable to result from the retention of those data, and, secondly, the seriousness of the interference entailed by such retention, it is necessary, within a democratic society, that retention be the exception and not the rule, as provided for in the system established by Directive 2002/58, and that those data should not be retained systematically and continuously. That conclusion applies even having regard to the objectives of combating serious crime and preventing serious threats to public security and to the

importance that must be attached to them (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 65 and the case-law cited).

108. Secondly, a targeted measure for the retention of traffic and location data may, at the choice of the national legislature and in strict compliance with the principle of proportionality, also be set using a geographical criterion where the competent national authorities consider, on the basis of objective and non-discriminatory factors, that there exists, in one or more geographical areas, a situation characterised by a high risk of preparation for or commission of serious criminal offences. Those areas may include places with a high incidence of serious crime, places that are particularly vulnerable to serious crime, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations, maritime ports or tollbooth areas (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 79 and the case-law cited).

122. In the fourth and final place, it must be emphasised that the proportionality of the measures adopted pursuant to Article 15(1) of Directive 2002/58 requires, according to the Court's settled case-law, as recalled in the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), compliance not only with the requirements of aptitude and of necessity but also with that of the proportionate nature of those measures in relation to the objective pursued (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 93).

***Ligue des droits humains v Conseil des ministres* (C-817/19), Judgment, Grand Chamber, Court of Justice of the European Union (21 June 2022)**

115. As regards observance of the principle of proportionality, the protection of the fundamental right to respect for private life at EU level requires, in accordance with settled case-law of the Court, that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue (Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 140, and judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 52 and the case-law cited).

116. More specifically, the question whether the Member States may justify a limitation on the rights guaranteed in Articles 7 and 8 of the Charter must be assessed by measuring the seriousness of the interference which such a limitation entails and by verifying that the importance of the objective of general interest pursued by that limitation is proportionate to that seriousness (see, to that effect, judgments of 2 October 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, paragraph 55 and the case-law cited, and of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 53 and the case-law cited).

117. In order to satisfy the proportionality requirement, the legislation in question entailing the interference must lay down clear and precise rules governing the scope and application of the measures provided for and imposing minimum safeguards, so that the persons whose data have been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data are subject to automated processing. Those considerations apply especially where the PNR data are liable to reveal sensitive passenger data (Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 141, and judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 132 and the case-law cited).

***Spetsializirana prokuratura* (C-350/21), Judgment, Court of Justice of the European Union (17 November 2022) (translated from the original French)**

64. Furthermore, while it is for national law to determine the conditions under which such access is to be granted, national legislation must, in order to satisfy the requirement of proportionality, lay down clear and precise rules governing the scope and application of the measure at issue and imposing minimum requirements, so that the persons whose personal data are concerned have sufficient safeguards to protect those data effectively against the risks of misuse. In particular, national legislation governing access by the competent authorities to stored traffic data and location data, adopted under Article 15(1) of Directive 2002/58, cannot be limited to requiring that access by the authorities to the data be in accordance with the purpose pursued by that legislation, but must also lay down the material and procedural conditions governing that use (see, to that effect, Case C-140/20 *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraphs 103 and 104, and the case-law cited).

***G.D. v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, and Attorney General*, (C-140/20), Judgment, Grand Chamber, Court of Justice of the European Union (5 April 2022)**

48. That being said, in so far as Article 15(1) of Directive 2002/58 allows Member States to introduce the derogations referred to in paragraph 34 to 37 of this judgment, that provision reflects the fact that the rights enshrined in Articles 7, 8 and 11 of the Charter are not absolute rights, but must be considered in relation to their function in society. Indeed, as can be seen from Article 52(1) of the Charter, that provision allows limitations to be placed on the exercise of those rights, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. Thus, in order to interpret Article 15(1) of Directive 2002/58 in the light of the Charter, account must also be taken of the importance of the rights enshrined in Articles 3, 4, 6 and 7 of the Charter and of the importance of the objectives of protecting national security and combating serious crime in contributing to the protection of the rights and freedoms of others (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 120 to 122 and the case-law cited).

49. Thus as regards, in particular, effective action to combat criminal offences committed against, inter alia, minors and other vulnerable persons, it should be borne in mind that positive obligations of the public authorities may result from Article 7 of the Charter, requiring them to adopt legal measures to protect private and family life. Such obligations may also arise from Article 7, concerning the protection of an individual's home and communications, and Articles 3 and 4, as regards the protection of an individual's physical and mental integrity and the prohibition of torture and inhuman and degrading treatment (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 126 and the case-law cited).

50. It is against the backdrop of those different positive obligations that the Court must strike a balance between the various interests and rights at issue. The European Court of Human Rights has held that the positive obligations flowing from Articles 3 and 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, whose corresponding safeguards are set out in Articles 4 and 7 of the Charter, require, in particular, the adoption of substantive and procedural provisions as well as practical measures enabling effective action to combat crimes against the person through effective investigation and prosecution, that obligation being all the more important when a child's physical and moral well-being is at risk. However, the measures to be taken by the competent authorities must fully respect due process and the other safeguards limiting the scope of criminal investigation powers, as well as other freedoms and rights. In particular, according to that court, a legal framework should be established enabling a balance to be struck between the various

interests and rights to be protected (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 127 and 128 and the case-law cited).

51. In that context, it is clear from the wording itself of the first sentence of Article 15(1) of Directive 2002/58 that the Member States may adopt a measure derogating from the principle of confidentiality referred to in paragraph 35 of this judgment where such a measure is 'necessary, appropriate and proportionate … within a democratic society', and recital 11 of the directive specifies, in that respect, that a measure of that nature must be 'strictly' proportionate to the intended purpose (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 129).

54. In order to satisfy the requirement of proportionality, the national legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that those data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data are subjected to automated processing, in particular where there is a significant risk of unlawful access to those data. Those considerations apply especially where the protection of the particular category of personal data that are sensitive data is at stake (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 132 and the case-law cited).

56. As regards the public interest objectives that may justify a measure taken pursuant to Article 15(1) of Directive 2002/58, it is clear from the Court's case-law, in particular the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), that, in accordance with the principle of proportionality, there is a hierarchy amongst those objectives according to their respective importance and that the importance of the objective pursued by such a measure must be proportionate to the seriousness of the interference that it entails.

57. In that regard, the Court held that the importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU according to which national security remains the sole responsibility of each Member State, exceeds that of the other objectives referred to in Article 15(1) of Directive 2002/58, inter alia the objectives of combating crime in general, even serious crime, and of safeguarding public security. Subject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives (see, to that effect, judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 135 and 136).

58. It is for that reason that the Court held that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, does not preclude legislative measures that allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists (judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168).

59. As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, the Court held that, in accordance with the principle of proportionality, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data. Accordingly, only non-serious interference with those fundamental rights may be justified by the objective of preventing, detecting and prosecuting criminal offences in general (judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 140 and the case-law cited).

79. Second, a targeted measure for the retention of traffic and location data may, at the choice of the national legislature and in strict compliance with the principle of proportionality, also be set using a geographical criterion where the competent national authorities consider, on the basis of objective and non-discriminatory factors, that there exists, in one or more geographical areas, a situation characterised by a high risk of preparation for or commission of serious criminal offences. Those areas may include places with a high incidence of serious crime, places that are particularly vulnerable to serious crime, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations, maritime ports or tollbooth areas (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 150 and the case-law cited).

93. In the fourth and final place, it must be emphasised that the proportionality of the measures adopted pursuant to Article 15(1) of Directive 2002/58 requires, according to the Court's settled case-law, as recalled in the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), compliance not only with the requirements of aptitude and of necessity but also with that of the proportionate nature of those measures in relation to the objective pursued.

***La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées ; Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministers (C-511/18, C-512/18 and C-520/18)*, Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2020)**

132. In order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subjected to automated processing, particularly where there is a significant risk of unlawful access to that data. Those considerations apply especially where the protection of the particular category of personal data that is sensitive data is at stake.

141. National legislation providing for the general and indiscriminate retention of traffic and location data for the purpose of combating serious crime exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society […].

150. The limits on a measure providing for the retention of traffic and location data may also be set using a geographical criterion where the competent national authorities consider, on the basis of objective and non-discriminatory factors, that there exists, in one or more geographical areas, a situation characterised by a high risk of preparation for or commission of serious criminal offences

[…]. Those areas may include places with a high incidence of serious crime, places that are particularly vulnerable to the commission of serious criminal offences, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations or tollbooth areas.

155. In those circumstances, while it is true that a legislative measure providing for the retention of the IP addresses of all natural persons who own terminal equipment permitting access to the Internet would catch persons who at first sight have no connection, within the meaning of the case-law cited in paragraph 133 of the present judgment, with the objectives pursued, and it is also true, in accordance with what has been stated in paragraph 109 of the present judgment, that Internet users are entitled to expect, under Articles 7 and 8 of the Charter, that their identity will not, in principle, be disclosed, a legislative measure providing for the general and indiscriminate retention of only IP addresses assigned to the source of a connection does not, in principle, appear to be contrary to Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, provided that that possibility is subject to strict compliance with the substantive and procedural conditions which should regulate the use of that data.

156. In the light of the seriousness of the interference entailed by that retention with the fundamental rights enshrined in Articles 7 and 8 of the Charter, only action to combat serious crime, the prevention of serious threats to public security and the safeguarding of national security are capable of justifying that interference. Moreover, the retention period must not exceed what is strictly necessary in the light of the objective pursued. Finally, a measure of that nature must establish strict conditions and safeguards concerning the use of that data, particularly via tracking, with regard to communications made and activities carried out online by the persons concerned.

158. It follows that, in accordance with what has been stated in paragraph 140 of the present judgment, legislative measures concerning the processing of that data as such, including the retention of and access to that data solely for the purpose of identifying the user concerned, and without it being possible for that data to be associated with information on the communications made, are capable of being justified by the objective of preventing, investigating, detecting and prosecuting criminal offences in general, to which the first sentence of Article 15(1) of Directive 2002/58 refers (see, to that effect, judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraph 62).

159. In those circumstances, having regard to the balance that must be struck between the rights and interests at issue, and for the reasons set out in paragraphs 131 and 158 of the present judgment, it must be held that, even in the absence of a connection between all users of electronic communications systems and the objectives pursued, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not preclude a legislative measure which requires providers of electronic communications services, without imposing a specific time limit, to retain data relating to the civil identity of all users of electronic communications systems for the purposes of preventing, investigating, detecting and prosecuting criminal offences and safeguarding public security, there being no need for the criminal offences or the threats to or acts having adverse effects on public security to be serious.

210. […] In particular, as is the case for Article 15(1) of Directive 2002/58, the power conferred on Member States by Article 23(1) of Regulation 2016/679 may be exercised only in accordance with the requirement of proportionality, according to which derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary […].

***Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service (C-623/17)*, Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2020)**

66. Concerning observance of the principle of proportionality, the first sentence of Article 15(1) of Directive 2002/58 provides that the Member States may adopt a measure derogating from the principle that communications and the related traffic data are to be confidential where such a measure is 'necessary, appropriate and proportionate … within a democratic society', in view of the objectives set out in that provision. Recital 11 of that directive specifies that a measure of that nature must be 'strictly' proportionate to the intended purpose.

68. In order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subjected to automated processing, in particular where there is a significant risk of unlawful access to that data. Those considerations apply especially where the protection of the particular category of personal data that is sensitive data is at stake […].

70. […] In that regard, it does not matter whether the information in question relating to persons' private lives is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference […].

71. The interference with the right enshrined in Article 7 of the Charter entailed by the transmission of traffic data and location data to the security and intelligence agencies must be regarded as being particularly serious, bearing in mind inter alia the sensitive nature of the information which that data may provide and, in particular, the possibility of establishing a profile of the persons concerned on the basis of that data, such information being no less sensitive than the actual content of communications. In addition, it is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance […].

73. Lastly, given the significant amount of traffic data and location data that can be retained continuously by a general retention measure and the sensitive nature of the information which that data may provide, the mere retention of that data by the providers of electronic communications services entails a risk of abuse and unlawful access.

78. Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the aim pursued, cannot be regarded as being limited to what is strictly necessary, national legislation governing access to traffic data and location data must rely on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data at issue […].

E. THE PRINCIPLE OF ADEQUATE SAFEGUARDS

UN General Assembly Resolution on Terrorism and Human Rights, UN Doc A/RES/78/210 (19 December 2023)*

30. *Urges* States to safeguard the right to privacy in accordance with international law, in particular international human rights law, and to take measures to ensure that interference with or restriction of that right are not arbitrary, are adequately regulated by law and are subject to effective oversight and appropriate redress, including through judicial review or other means;

** See also UN General Assembly Resolution on Terrorism and Human Rights, UN Doc A/RES/74/147 (18 December 2019); UN General Assembly Resolution on Terrorism and Human*

Rights, UN Doc A/RES/73/174 (17 December 2018)

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

10. Calls upon all States: (c) To review, on a regular basis, their procedures, practices and legislation regarding the surveillance of communications, including mass surveillance and the interception and collection of personal data, as well as regarding the use of profiling, automated decision-making, machine learning and biometric technologies, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

** See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021)*

Concluding Observations on Equatorial Guinea in the Absence of Its Initial Report, Human Rights Committee, UN Doc CCPR/C/GNQ/CO/1 (22 August 2019)

51. The State party should ensure: (b) that surveillance and interception are subject to judicial authorization, and to effective and independent oversight mechanisms;

***Weber and Saravia v Germany*, App No 54934/00, Decision, European Court of Human Rights (29 June 2006)**

95. In the case-law on secret measures of surveillance the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019)

6. *Calls upon* all States: (f) To put in place adequate safeguards seeking to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services, including where necessary through contractual clauses, and promptly inform relevant domestic, regional or international oversight bodies of abuses or violations when misuse of their products and services is detected;

Concluding Observations on the Second Periodic Report of Indonesia, Human Rights Committee, UN Doc CCPR/C/IDN/CO/2 (26 March 2024)

13. The State party should: (b) ensure that any restrictions, such as wiretapping, to the right to privacy of individuals suspected of, or charged with, terrorist acts are subject to judicial review and effective, regular and independent oversight, while guaranteeing access to effective remedies in case of abuse of authority;

Concluding Observations on the Eighth Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/8 (26 March 2024)

51. […] [T]he Committee urges the State party to ensure that proposals in the Investigatory Powers (Amendment Bill and the Data Protection and Digital Information Bill apply strict safeguards and oversight, including judicial review, in compliance with international standards. […]

Concluding Observations on the Fifth Periodic Report on the Philippines, Human Rights Committee, UN Doc CCPR/C/PHL/CO/5 (28 October 2022)

42. The State party should ensure that all types of data retention and access and any arbitrary and unlawful interference with privacy, including in the context of the Government's anti-illegal drug campaign, are in full conformity with the Covenant, in particular article 17 thereof. Such acts should comply with the principles of legality, proportionality and necessity and be subject to judicial authorization. The State party should ensure prompt, independent and effective investigations into all cases of abuse and provide victims with access to effective remedies.

Concluding Observations on the Fifth Periodic Report of the Netherlands, Human Rights Committee, UN Doc CCPR/C/NLD/CO/5 (22 August 2019)

54. The Committee is concerned about the Intelligence and Security Services Act 2017, which provides the intelligence and security services with sweeping surveillance and interception powers, including bulk data collection. It is particularly concerned that the Act does not provide for a clear definition of case-specific bulk data collection; clear grounds for extending retention periods for information collected; and adequate safeguards against bulk data hacking. It is also concerned by the limited practical possibilities for complaining, in the absence of a comprehensive notification regime, to the Review Committee on the Intelligence and Security Services (art. 17).

55. The State party should review the Act with a view to bringing its definitions and the powers and limits on their exercise in line with the Covenant and strengthen the independence and effectiveness of the two new bodies established by the Act, the Evaluation Committee on the Use of Powers and the Review Committee on the Intelligence and Security Services."

Concluding Observations on the Fifth Periodic Report of Belarus, Human Rights Committee, UN Doc CCPR/C/BLR/CO/5 (22 November 2018)

44. The State party should ensure that: […] (b) surveillance and interception is conducted subject to judicial authorization as well as effective and independent oversight mechanisms; […]"

Concluding Observations on the Sixth Periodic Report of Hungary, Human Rights Committee, UN Doc CCPR/C/HUN/CO/6 (9 May 2018)

43. The Committee is concerned that the State party's legal framework on secret surveillance for national security purposes (section 7/E (3) surveillance): […] (b) contains insufficient safeguards against arbitrary interference with the right to privacy. […]

44. The State party should increase the transparency of the powers of the legal framework on secret surveillance for national security purposes (section 7/E (3) surveillance) and the safeguards against its abuse by considering the possibility of making its policy guidelines and decisions public, in full or in part, subject to national security considerations and the privacy interests of individuals concerned by those decisions. It should ensure [...] that effective and independent oversight mechanisms for secret surveillance are put in place; and that the persons affected have proper access to effective remedies in cases of abuse.

Concluding Observations on the Second Periodic Report of Turkmenistan, Human Rights Committee, UN Doc CCPR/C/TKM/CO/2 (28 March 2017)

37. The State party should ensure that: (b) surveillance is subject to judicial authorization as well as effective and independent oversight mechanisms;

Concluding Observations on the Initial Report of South Africa, Human Rights Committee, UN Doc CCPR/C/ZAF/CO/1 (27 April 2016)

42. The Committee is concerned about the relatively low threshold for conducting surveillance in the State party and the relatively weak safeguards, oversight and remedies against unlawful interference with the right to privacy contained in the 2002 Regulation of Interception of Communications and Provision of Communication-Related Information Act. [...]

43. […] It should also ensure that interception of communications by law enforcement and security services is carried out only according to the law and under judicial supervision. The State party should increase the transparency of its surveillance policy and speedily establish independent oversight mechanisms to prevent abuses and ensure that individuals have access to effective remedies.

Concluding Observations on the Second Periodic Report of Namibia, Human Rights Committee, UN Doc CCPR/C/NAM/CO/2 (22 April 2016)

38. The State party should ensure that the interception of telecommunication s may only be justified under limited circumstances authorized by law with the necessary procedural and judicial safeguards against abuse, and supervised by the courts when in full conformity with the Covenant.

Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, UN Doc CCPR/C/USA/CO/4, (23 April 2014)

22. Reform the current oversight system of surveillance activities to ensure its effectiveness, including by providing for judicial involvement in the authorization or monitoring of surveillance measures, and considering the establishment of strong and independent oversight mandates with a view to preventing abuses.

***Podchasov v Russia*, App No 33696/19, Judgment, European Court of Human Rights (13 February 2024)**

62. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes (see *S. and Marper*, cited above, § 103, and, in the context of bulk interception of communications, *Big Brother Watch and Others*, cited above, § 330), and especially where the technology available is continually becoming more sophisticated (see, in the context of storage of personal data, *Uzun v. Germany*, no. 35623/05, § 61, ECHR 2010 (extracts); *Catt v. the United Kingdom*, no. 43514/15, § 114, 24 January 2019; and *Gaughran v. the United Kingdom*, no. 45245/15, § 86, 13 February 2020; see also, in the context of secret surveillance, *Roman Zakharov*, § 229, and *Big Brother Watch and Others,* § 333, both cited above). The protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern technologies in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such technologies against important private-life interests (see, *mutatis mutandis*, *S. and Marper*, cited above, § 112).

74. […] In [the *Zakharov*] case the Court found that Russian legal provisions governing secret surveillance measures did not meet the "quality of law" requirement because they did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse. They were therefore incapable of keeping the "interference" to what was "necessary in a democratic society". It found, in particular, that the circumstances in which public authorities were empowered to resort to secret surveillance measures for the purposes of detecting, preventing and investigating criminal offences or protecting Russia's national, military, economic or ecological security were not defined with sufficient clarity. The authorisation procedures were not capable of ensuring that secret surveillance measures were ordered only when "necessary in a democratic society". The supervision of interceptions did not comply with the requirements of independence, powers and competence which were sufficient to exercise effective and continuous control, public scrutiny and effectiveness in practice. The effectiveness of the remedies was undermined by the absence of notification at any point of secret surveillance, or adequate access to documents relating to secret surveillance (see *Roman Zakharov*, cited above, §§ 243-305).

75. The Court does not see any reason to reach a different conclusion in the present case. It therefore finds that the domestic law does not provide for adequate and sufficient safeguards against abuse relating to the access by the law-enforcement authorities to the Internet communications and related communications data stored by ICOs pursuant to the Information Act.

***N.F. and Others v Russia*, Apps Nos 3537/15 and 8 others, Judgment, European Court of Human Rights (12 September 2023)**

45. […] The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for his private life, as guaranteed by Article 8 of the Convention. The domestic law must therefore afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article (see *P.N. v. Germany*, no. 74440/17, § 70, 11 June 2020, and *S. and Marper*, cited above, § 103). The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should in particular ensure that such data are relevant and not excessive in relation to the purposes for which they are stored, and are preserved in a form that permits the identification of the data subjects for no longer than is required for the purpose for which those data are stored. The domestic law must also afford adequate guarantees that retained personal data shall be efficiently protected from misuse and abuse (see *P.N. v. Germany*, cited above, § 71, with further references).

***Ekimdzhiev and Ors v Bulgaria*, App No 70078/12, Judgment, European Court of Human Rights (11 January 2022)**

292. […] a secret surveillance system must contain effective guarantees – especially review and oversight arrangements – which protect against the inherent risk of abuse and which keep the interference which such a system entails with the rights protected by Article 8 of the Convention to what is "necessary in a democratic society".

293. In cases such as the present one, in which the applicants complain in the abstract about a system of secret surveillance rather than of specific instances of such surveillance, the relevant national laws and practices are to be scrutinised as they stand when the Court examines the admissibility of the application rather than as they stood when it was lodged (see *Centrum för rättvisa*, § 151, and *Big Brother Watch and Others*, § 270, both cited above). The other point of particular relevance to this case is that the assessment of whether the laws at issue offer effective guarantees must be based not only the laws as they exist in the statute book, but also on (a) the actual operation of the surveillance regime, and (b) the existence or absence of evidence of actual abuse (see *Centrum för rättvisa*, § 274, and *Big Brother Watch and Others*, § 360, both cited above).

308. The relevant legislation in Bulgaria lays down robust safeguards intended to ensure that secret surveillance is resorted to only when that is truly justified. First, only a limited number of authorities can request surveillance, within the spheres of their respective competencies (see paragraphs 32 to 36 above). Secondly, the law appears to provide for a form of internal review preceding the submission of surveillance applications: those made by executive authorities must originate from the head of the respective authority, and public prosecutors intending to make such applications must notify their hierarchical superiors (see paragraph 37 above). Thirdly and most importantly, surveillance may be authorised only by the competent court president or an expressly authorised deputy (see paragraphs 46 and 47 above). Lastly, the authority which carries out the surveillance must, before proceeding with it, scrutinise the surveillance application for incompatibility *ratione materiae* or obvious mistakes and, if it spots issues in those respects, refer the application back to the judge who authorised the surveillance for reconsideration (see paragraph 73 above).

310. […] But it must also be seen whether those safeguards are being properly applied in practice.

321. It follows that the Court cannot be satisfied that the procedures for authorising secret surveillance, as operating in practice in Bulgaria, effectively guarantee that such surveillance is authorised only when genuinely necessary and proportionate in each case (compare with Roman Zakharov, cited above, §§ 262-63).

***Ivashchenko v Russia*, App No 61064/10, Judgment, European Court of Human Rights (13 February 2018)**

76. […] As regards the latter point, the Court must firstly ensure that the relevant legislation and practice afford individuals "adequate and effective safeguards against abuse"; notwithstanding the margin of appreciation which the Court recognises the Contracting States have in this sphere, it must be particularly vigilant where the authorities are empowered under national law to order and effect searches without a judicial warrant. If individuals are to be protected from arbitrary interference by the authorities with the rights guaranteed under Article 8, a legal framework and very strict limits on such powers are called for. […]

81. […] In the Court's view and for the reasons presented below, the safeguards provided by Russian law have not been demonstrated as constituting an adequate framework for the wide powers afforded to the executive which could offer individuals adequate protection against arbitrary interference.

***Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, App No 62540/00, Judgment, European Court of Human Rights (28 June 2007)**

92. [...] the Court notes that the Bulgarian Supreme Cassation Prosecutor's Office apparently found, in a report of January 2001, that numerous abuses had taken place. According to this report, more than 10,000 warrants were issued over a period of some twenty-four months, from 1 January 1999 to 1 January 2001, and that number does not even include the tapping of mobile telephones (for a population of less than 8,000,000). Out of these, only 267 or 269 had subsequently been used in criminal proceedings. A significant number of breaches of the law had been observed. Additionally, in an interview published on 26 January 2001 the then Minster of Internal Affairs conceded that he had signed 4,000 orders for the deployment of means of secret surveillance during his thirteen months in office. By contrast, in *Malone*, the number of the warrants issued was considered relatively low (400 telephone tapping warrants and less than 100 postal warrants annually during the period 1969-79, for more than 26,428,000 telephone lines nationwide). These differences are telling, even if allowance is made for the development of the means of communication and the rise in terrorist activities in recent years. They also show that the system of secret surveillance in Bulgaria is, to say the least, overused, which may in part be due to the inadequate safeguards which the law provides.

***Kopp v Switzerland*, App No 23224/94, Judgment, European Court of Human Rights (25 March**

1998)

71. […] [The Government] added that Mr Kopp, the husband of a former member of the Federal Council, had not had his telephones tapped in his capacity as a lawyer. In the instant case, in accordance with Swiss telephone-monitoring practice, a specialist Post Office official had listened to the tape in order to identify any conversations relevant to the proceedings in progress, but no recording had been put aside and sent to the Federal Public Prosecutor's Office.

***Leander v Sweden*, App No 9248/81, Judgment, European Court of Human Rights (26 March 1987)**

60. [...] in view of the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse.

***Klass and Others v Germany*, App No 5029/71, Judgment, European Court of Human Rights (6 September 1978)**

50. The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law […]

59. Both in general and in relation to the question of subsequent notification, the applicants have constantly invoked the danger of abuse as a ground for their contention that the legislation they challenge does not fulfil the requirements of Article 8 para. 2 (art. 8-2) of the Convention. While the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system, the considerations that matter for the purposes of the Court's present review are the likelihood of such action and the safeguards provided to protect against it. The Court has examined above the contested legislation in the light, inter alia, of these considerations. The Court notes in particular that the G 10 contains various provisions designed to reduce the effect of surveillance measures to an unavoidable minimum and to ensure that the surveillance is carried out in strict accordance with the law. In the absence of any evidence or indication that the actual practice followed is otherwise, the Court must assume that in the democratic society of the Federal Republic of Germany, the relevant authorities are properly applying the legislation in issue. The Court agrees with the Commission that some compromise between the requirements for defending democratic society and individual rights is inherent in the system of the Convention. As the Preamble to the Convention states, "Fundamental Freedoms [...] are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the Human Rights upon which (the Contracting States) depend". In the context of Article 8 (art. 8), this means that a balance must be sought between the exercise by the individual ofthe right guaranteed to him under paragraph 1 (art. 8-1) and the necessity under paragraph 2 (art. 8-2) to impose secret surveillance for the protection of the democratic society as a whole.

African Commission on Human and Peoples' Rights, Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa, ACHPR/Res.573 (LXXVII) (9 November 2023)

Underscoring Principle 41 of the Declaration which provides that States should only engage in targeted surveillance in conformity with international human rights law and ensure that any law authorizing targeted communication surveillance provides adequate safeguards for the right to privacy, and Principle 42(7) which provides that "every individual shall have legal recourse to

effective remedies in relation to the violation of their privacy and the unlawful processing of their personal information;"

The African Commission calls on States Parties to: ii. Align approaches on the regulation of communication surveillance with relevant international human rights law and standards, considering safeguards such as the requirement for prior authorization by an independent and impartial judicial authority and the need for effective monitoring and regular review by independent oversight mechanisms;

***Ligue des droits humains v Conseil des ministres* (C-817/19), Judgment, Grand Chamber, Court of Justice of the European Union (21 June 2022)**

189. As regards the requirements which those databases must satisfy, it is appropriate to note that, under Article 6(4) of the PNR Directive, advance assessment against pre-determined criteria must, pursuant to Article 6(3)(b) of that directive, be carried out in a non-discriminatory manner, those criteria must be targeted, proportionate and specific, and must be set and regularly reviewed by the PIUs in cooperation with the competent authorities referred to in Article 7 of the directive. If, by referring to Article 6(3)(b) of that directive, the wording of Article 6(4) thereof covers only the processing of PNR data against pre-determined criteria, the latter provision must be interpreted, in the light of Articles 7, 8 and 21 of the Charter, as meaning that the requirements it lays down apply mutatis mutandis to the comparison of those data against the databases referred in the preceding paragraph, especially since those requirements correspond, in essence, to those adopted by the case-law arising from Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592, paragraph 172), for the purposes of cross-checking PNR data against databases.190In that regard, it should be stated that the requirement as to the non-discriminatory nature of those databases implies, inter alia, that entry into the databases on persons sought or under alert is based on objective and non-discriminatory factors, defined in EU, international and national rules applicable to such databases (see, by analogy, judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 78).191In addition, in order to satisfy the requirement as to the targeted, proportionate and specific nature of the pre-determined criteria, the databases referred to in paragraph 188 above must be used in relation to the fight against terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.192Moreover, the databases used pursuant to Article 6(3)(a) of the PNR Directive must, in view of the considerations set out in paragraphs 183 and 184 above, be managed by the competent authorities referred to in Article 7 of that directive or, with regard to EU databases as well as international databases, be exploited by those authorities in the context of their mission to combat terrorist offences and serious crime. That is the case of the databases on persons or objects sought or under alert, in accordance with the EU, international and national rules applicable to such databases.

(5) (ii) Processing PNR data against pre-determined criteria

199. In order to target in that way the persons thus referred to and given the risk of discrimination that criteria based on the characteristics set out in the fourth sentence of Article 6(4) of the PNR Directive entail, the PIU and the competent authorities cannot, generally, rely on those characteristics. By contrast, as pointed out by the German Government at the hearing, they can inter alia take into consideration specific features in the factual conduct of persons when preparing and engaging in air travel which, following the findings of and experience acquired by the competent authorities, might suggest that the persons acting in that way may be involved in terrorist offences or serious crime.

200. In that context, as noted by the Commission in response to a question put by the Court, pre-determined criteria must be defined in such a way as to take into consideration both 'incriminating' as well as 'exonerating' circumstances, since that requirement may contribute to the reliability of

those criteria and, in particular, ensure that they are proportionate, as required by the second sentence Article 6(4) of the PNR Directive.

201. Lastly, the third sentence of Article 6(4) of that directive provides that pre-determined criteria must be reviewed regularly. In the context of that review, those criteria must be updated in accordance with changes in the circumstances that justified their being taken into consideration for the purposes of advance assessment, thus making it possible, inter alia, to react to developments in the fight against terrorist offences and serious crime referred to in paragraph 157 above (see, by analogy, judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 82). In particular, that review must take into account the experience acquired in the context of the application of pre-determined criteria, in order to reduce, as much as possible, the number of 'false positives' and, thereby, contribute to the strictly necessary nature of the application of those criteria.

(5)(iii) Safeguards surrounding the automated processing of PNR data

203. As regards pre-determined criteria specifically, it is appropriate, first of all, to specify that, although the PIU, as stated in recital 7 of the PNR Directive, must define the assessment criteria in a manner which keeps to a minimum the number of innocent people wrongly identified by the system established by that directive, that unit must still, in accordance with Article 6(5) and (6) of the said directive, individually review any positive match by non-automated means in order to identify, as much as possible, any 'false positives'. In addition, notwithstanding the fact that they must set the assessment criteria in a non-discriminatory manner, the PIU is required to carry out such a review for the purposes of excluding any discriminatory results. The PIU must comply with that same review obligation when comparing PNR data against databases.

205. As regards the verifications which the PIU must carry out to that end, it follows from Article 6(5) and (6) of the PNR Directive, read in conjunction with recitals 20 and 22 thereof, that Member States must lay down clear and precise rules capable of providing guidance and support for the analysis carried out by the agents in charge of the individual review, for the purposes of ensuring full respect for the fundamental rights enshrined in Articles 7, 8 and 21 of the Charter and, in particular, guarantee a uniform administrative practice within the PIU that observes the principle of non-discrimination.

206. In particular, given the fairly substantial number of 'false positives', mentioned in paragraph 106 above, Member States must ensure that the PIU establishes, in a clear and precise manner, objective review criteria enabling its agents to verify, on the one hand, whether and to what extent a positive match ('hit') concerns effectively an individual who may be involved in the terrorist offences or serious crime referred to in paragraph 157 above and must, therefore, be subject to further examination by the competent authorities referred to Article 7 of that directive, as well as, on the other hand, the non-discriminatory nature of automated processing operations under that directive and, in particular, the pre-determined criteria and databases used.

207. In that context, Member States are required to ensure that, in accordance with Article 13(5) of the PNR Directive, read in conjunction with recital 37 thereof, the PIUs maintain documentation relating to all processing of PNR data carried out in connection with the advance assessment, including in the context of the individual review by non-automated means, for the purpose of verifying its lawfulness and for the purpose of self-monitoring.

208. Next, the competent authorities, pursuant to the first sentence of Article 7(6) of the PNR Directive, cannot take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data, which means, in connection with the advance assessment, that they must take into consideration and, where applicable, give preference to the result of the individual review conducted by non-automated means

by the PIU over that obtained by automated processing. The second sentence of that Article 7(6) specifies that those decisions must not be discriminatory.

209. In that context, the competent authorities must ensure the lawfulness of the automated processing, in particular its non-discriminatory nature, as well as that of the individual review.

211. Lastly, in the context of redress introduced pursuant to Article 13(1) of the PNR Directive, the court responsible for reviewing the legality of the decision adopted by the competent authorities as well as, except in the case of threats to State security, the persons concerned themselves must have had an opportunity to examine both all the grounds and the evidence on the basis of which the decision was taken (see, by analogy, judgment of 4 June 2013, ZZ, C-300/11, EU:C:2013:363, paragraphs 54to 59), including the pre-determined assessment criteria and the operation of the programs applying those criteria.

I. REASONABLE SUSPICION

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

61. The High Commissioner recommends that States: […] (e) […] clarify that authorization of surveillance measures requires reasonable suspicion that a particular individual has committed or is committing a criminal offence or is engaged in acts amounting to a specific threat to national security;

***Roman Zakharov v Russia*, App No 47143/06, Judgment, European Court of Human Rights (4 December 2015)**

260. Turning now to the authorisation authority's scope of review, the Court reiterates that it must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security. It must also ascertain whether the requested interception meets the requirement of "necessity in a democratic society", as provided by Article 8 § 2 of the Convention, including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means.

***Klass and Others v Germany*, App No 5029/71, Judgment, European Court of Human Rights (6 September 1978)**

51. According to the G 10, a series of limitative conditions have to be satisfied before a surveillance measure can be imposed. Thus, the permissible restrictive measures are confined to cases in which there are factual indications for suspecting a person of planning, committing or having committed certain serious criminal acts; measures may only be ordered if the establishment of the facts by another method is without prospects of success or considerably more difficult; even then, the surveillance may cover only the specific suspect or his presumed "contact-persons". Consequently, so-called exploratory or general surveillance is not permitted by the contested legislation. Surveillance may be ordered only on written application giving reasons, and such an application may be made only by the head, or his substitute, of certain services; the decision thereon must be taken by a Federal Minister empowered for the purpose by the Chancellor or, where appropriate, by the supreme Land authority. Accordingly, under the law there exists an administrative procedure designed to ensure that measures are not ordered haphazardly, irregularly or without due and proper consideration. In addition, although not required

by the Act, the competent Minister in practice and except in urgent cases seeks the prior consent of the G 10 Commission.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights while Counter-Terrorism, Human Rights Implications of the Development, Use, Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism, UN Doc A/HRC/52/39 (1 March 2023)

39. […] The Special Rapporteur highlights her profound disquiet at AI assessments being used to trigger State action in counter-terrorism contexts, from searching, questioning, arrest, prosecution and administrative measures to deeper, more intrusive surveillance, when AI assessments alone should not be the basis for reasonable suspicion given its inherently probabilistic nature. […]

Concluding Observations on the Seventh Periodic Report of Norway, Human Rights Committee, UN Doc CCPR/C/NOR/CO/7 (25 April 2018)

20. The Committee is concerned that amendments to the Code of Criminal Procedure and Police Act in 2016 grant broader monitoring and search powers to police, which may be used in a preventative manner to anticipate crime and may lack sufficient safeguards to prevent interference with the right to privacy. It is also concerned at reports about the intrusive use of satellite communications and of an ongoing proposal for a system of bulk data retention and its implications for the right to privacy (art. 17).

***Svetova and Others v Russia*, App No 54714/17, Judgment, European Court of Human Rights (24 January 2023)**

39. The Court finds no indication that the applicants were charged with or suspected of any criminal offence or unlawful activities. Their home was searched in connection with a criminal case against third parties in which the applicants did not have any procedural status. In the absence of a copy of the search warrant and the domestic courts' findings, the Court is unable to satisfy itself that the warrant was based on a reasonable suspicion that any items indicative of any criminal activities might be found in the applicants' flat (compare *Misan*, cited above, §§ 56-57). The reasons indicated in the search record which appear to reflect the language of the search warrant (see paragraph 18 above) cannot be accepted as "relevant" or "sufficient" as they did not indicate any possible connection between the applicants and the criminal case against the third parties.

***Liblik and Others v Estonia*, Apps Nos 173/15 and 5 others, Judgment, European Court of Human Rights (28 May 2019)**

136. The Court has also underlined the importance of an authority empowered to authorise the use of secret surveillance being capable of verifying "the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures" and "whether the requested interception meets the requirement of 'necessity in a democratic society' [...] for example, whether it is possible to achieve the aims by less restrictive means" […]."

***Gorlov and Others v Russia*, App No 27057/06, Judgment, European Court of Human Rights (2 July 2019)**

96. In the present case, however, the applicants' placement under permanent video surveillance was not based on an individualised and reasoned decision providing reasons which would have justified the measure in question in the light of the legitimate aims pursued; the contested measure

was not limited in time, and the administrations of the penal institutions or pre-trial detention centre as the case may be were not under an obligation to review regularly (or at all) the well-foundedness of that measure. Indeed, there does not appear to exist any basis in national law for the adoption of such individualised decisions, the Supreme Court of Russia noting in its decision of 12 March 2014 that the existing legal framework "[did] not provide for the adoption of any [individualised] decision [authorising] the use of technical means of control and supervision" […]."

***Ivashchenko v Russia*, App No 61064/10, Judgment, European Court of Human Rights (13 February 2018)**

84. […] the Court is not convinced that in order to avoid arbitrariness it was indispensable for the customs officer to have a reasonable suspicion of criminal activity *stricto sensu* (as being in breach of the Criminal Code of the Russian Federation), that is some objective basis for suspecting the particular person of "criminal" activity in the particular circumstances of a given situation taken as a whole. By way of comparison, the Court reiterates that it is also possible to envisage a justified interference with Article 8 rights by way of search-and-seizure or comparable measures in contexts other than those of a criminal investigation, in relation to unlawful conduct punishable under other procedures […]

86. In the context of the present case the Court is not convinced by the Government's submission that the fact that the applicant was returning from a disputed area constituted in itself a sufficient basis for proceeding with the extensive examination and copying of his electronic data on account of possible "extremist" content."

Dudchenko v Russia*, App No 37717/05, Judgment, European Court of Human Rights (7 November 2017)

97. […] Although the court noted, without any further details, that the police had "intelligence information" that the applicant was the leader of a gang and planned to commit extortions, it did not mention any facts or information that would satisfy an objective observer that the applicant might have committed or planned the offences. There is no evidence that any information or documents confirming the suspicion against the applicant had actually been submitted to the judge. […]

99. To sum up, the Court finds that the domestic court that authorised covert surveillance measures against the applicant did not verify whether there was a "reasonable suspicion" against him […]

**See also repeated in Moskalev v Russia, App No 44045/05, Judgment, European Court of Human Rights (7 November 2017), paras 36-45; Zubkov and others v Russia, App No 29431/05 and 2 others, Judgment, European Court of Human Rights (7 November 2017), paras 123-128*

***S. and Marper v The United Kingdom*, Apps Nos 30562/04 and 30566/04, Judgment, European Court of Human Rights (4 December 2008)**

122. Of particular concern in the present context is the risk of stigmatisation, stemming from the fact that persons in the position of the applicants, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons. In this respect, the Court must bear in mind that the right of every person under the Convention to be presumed innocent includes the general rule that no suspicion regarding an accused's innocence may be voiced after his acquittal. […]"

***Weber and Saravia v Germany*, App No 54934/00, Decision, European Court of Human Rights (29 June 2006)**

125. The Court finds that the transmission of personal data obtained by general surveillance measures without any specific prior suspicion in order to allow the institution of criminal proceedings

against those being monitored constitutes a fairly serious interference with the right of these persons to secrecy of telecommunications.

***La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées; Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministers (C-511/18, C-512/18 and C-520/18)*, Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2020)**

192. […] recourse to the real-time collection of traffic and location data is limited to persons in respect of whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities and is subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding in order to ensure that such real-time collection is authorised only within the limits of what is strictly necessary. In cases of duly justified urgency, the review must take place within a short time.

212. […] Article 23(1) of Regulation 2016/679, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which requires that providers of access to online public communication services and hosting service providers retain, generally and indiscriminately, inter alia, personal data relating to those services.

228. Article 15(1), interpreted in the light of the principle of effectiveness, requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact.

African Commission on Human and Peoples' Rights, Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa, ACHPR/Res.573 (LXXVII) (9 November 2023)

The African Commission calls on States Parties to: iii. Only engage in targeted communication surveillance that is authorized by law, that conforms with international human rights law and standards, and premised on reasonable suspicion that a serious crime has been or is being carried out.

II. JUDICIAL AUTHORISATION

The review of pronouncements by different human rights monitoring mechanisms shows that there are significant overlaps in references to the requirements of judicial authorization and effective oversight. It may therefore be pertinent to consult both sub-chapters. Reference to the requirement of judicial authorisation within the broader framework of adequate safeguards accompanying surveillance can be found in the introductory sub-chapter E.

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

39. Surveillance measures, including communications data requests to business enterprises and

intelligence-sharing, should be authorized, reviewed and supervised by independent bodies at all stages, including when they are first ordered, while they are being carried out and after they have been terminated (see CCPR/C/FRA/CO/5, para. 5). The independent body authorizing particular surveillance measures, preferably a judicial authority, needs to make sure that there is clear evidence of a sufficient threat and that the surveillance proposed is targeted, strictly necessary and proportionate and authorize (or reject) ex ante the surveillance measures.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

50. As a primary step, Governments deploying surveillance tools must ensure that they do so in accordance with a domestic legal framework that meets the standards required by international human rights law. Surveillance should only be authorised in law for the most serious criminal offences. To be compliant with those standards, national laws must:

(c) Ensure that a surveillance operation be approved for use against a specific person only in accordance with international human rights law and when authorized by a competent, independent and impartial judicial body, with all appropriate limitations on time, manner, place and scope of the surveillance;

(d) Require, given the extreme risks of abuse associated with targeted surveillance technologies, that authorized uses be subjected to detailed record-keeping requirements. Surveillance requests should only be permitted in accordance with regular, documented legal processes and the issuance of warrants for such use. Surveillance subjects should be notified of the decision to authorize their surveillance as soon as such a notification would not seriously jeopardize the purpose of the surveillance

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014)

45. One of the core protections afforded by article 17 is that covert surveillance systems must be attended by adequate procedural safeguards to protect against abuse. These safeguards may take a variety of forms, but generally include independent prior authorization and/or subsequent independent review. Best practice requires the involvement of the executive, the legislature and the judiciary, as well as independent civilian oversight [...]

46. Where targeted surveillance programmes are in operation, many States make provision for prior judicial authorization. Judicial involvement that meets international standards is an important safeguard, although there is evidence that in some jurisdictions the degree and effectiveness of such scrutiny has been circumscribed by judicial deference to the executive [...]

47. In the context of targeted surveillance, whichever method of prior authorization is adopted (judicial or executive), there is at least an opportunity for ex ante review of the necessity and proportionality of a measure of intrusive surveillance by reference to the particular circumstances of the case and the individual or organization whose communications are to be intercepted. Neither of these opportunities exists in the context of mass surveillance schemes since they do not depend on individual suspicion. Ex ante review is thus limited to authorizing the continuation of the scheme as a whole, rather than its application to a particular individual [...]

61. States should establish strong and independent oversight bodies that are adequately resourced and mandated to conduct ex ante review, considering applications for authorization not only against the requirements of domestic law, but also against the necessity and proportionality requirements of the Covenant. […]

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

There is particular interest in the creation of "public interest advocacy" positions within surveillance authorization processes. Given the growing role of third parties, such as Internet service providers, consideration may also need to be given to allowing such parties to participate in the authorization of surveillance measures affecting their interests or allowing them to challenge existing measures. The utility of independent advice, monitoring and/or review to help to ensure strict scrutiny of measures imposed under a statutory surveillance regime has been highlighted positively in relevant jurisprudence. Parliamentary committees also can play an important role; however, they may also lack the independence, resources or willingness to discover abuse, and may be subject to regulatory capture.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

50. To be compliant with those standards, national laws must: (c) Ensure that a surveillance operation be approved for use against a specific person only in accordance with international human rights law and when authorized by a competent, independent and impartial judicial body, with all appropriate limitations on time, manner, place and scope of the surveillance;"

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc A/HRC/13/37 (28 December 2009)

51. Surveillance systems require effective oversight to minimize harm and abuses. Where safeguard exist, this has traditionally taken the form of an independent authorization through a judicial warrant and/or a subpoena process with the opportunity of independent review. […]

Concluding Observations on the Fourth Periodic Report of Serbia, Human Rights Committee, UN Doc CCPR/C/SRB/CO/4 (26 March 2024)

37. The State party should ensure that adequate legal safeguards, including judicial review, are in place for its surveillance regime, including online surveillance, […]

Concluding Observations on the Third Periodic Report of Namibia, Human Rights Committee, UN Doc CCPR/C/NAM/CO/3 (22 March 2024)

31. […] [The State party] should also ensure that the management of the database for SIM card registration is subject to appropriate safeguards in order to prevent hacking, data leaks and unauthorized access by private entities and State authorities, including by establishing appropriate judicial or legislative authorization requirements for State authorities wishing to obtain access to the database.

Concluding Observations on the Fifth Periodic Report of the Republic of Korea, Human Rights Committee, UN Doc CCPR/C/KOR/CO/5 (30 October 2023)

49. The Committee is concerned about the lack of sufficient safeguards against arbitrary interference with the right to privacy in the State party's legislation, owing, inter alia, to the wide powers granted to security and law enforcement agencies to monitor Internet traffic, to access all subscriber information, and to intercept communications and retrieve data without a court order. The Committee takes note of the December 2022 amendment to the Protection of Communications Secrets Act, to require that investigative agencies apply to the court for permission in the context of emergency

surveillance and interception activities, but observes that this requirement applies only ex post (arts. 17, 19 and 21).

50. The State party should: (b) Ensure that surveillance and interception are subject to judicial authorization ex ante and to effective and independent oversight mechanisms;

Concluding Observations on the Initial Report of the State of Palestine, UN Doc CCPR/C/PSE/CO/1 (21 July 2023)

38. In the light of the Committee's general comment No. 16 (1988) on right to privacy, the State party should: (a) Ensure that any interference with the right to privacy, including activities carried out by the Preventive Security Service under Decree-Law No. 10 of 2018 regarding cybercrime, is subject to judicial review and to effective and independent oversight mechanisms;

Concluding Observations on the Second Periodic Report of Uganda, Human Rights Committee, UN Doc CCPR/C/UGA/CO/2 (20 July 2023)

17. The State party should take steps to ensure that counter-terrorism legislation is not used to unjustifiably limit any rights enshrined in the Covenant, including the rights to […] privacy, […]. It should […] ensure independent oversight of law enforcement and security forces in the context of counter-terrorism measures, including judicial review.

Concluding Observations on the Fourth Periodic Report of Zambia, Human Rights Committee, UN Doc CCPR/C/ZMB/CO/4 (20 March 2023)

32. […] The State party should also ensure that surveillance activities are subject to effective judicial oversight mechanisms and ensure access to effective remedies in cases of abuse.

Concluding Observations on the Fourth Periodic Report of Nicaragua, Human Rights Committee, UN Doc CCPR/C/NIC/CO/4 (31 October 2022)

32. […] the Committee urges the State party to: (c) […] ensure that the surveillance and interception of communications are subject to judicial authorization and that the individuals concerned have adequate access to effective remedies.

Concluding Observations on the Fifth Periodic Report of the Philippines, Human Rights Committee, UN Doc CCPR/C/PHL/CO/5 (28 October 2022)

14. The State party should: […] (d) Ensure that any interference with the right to privacy, including through the publication of the personal data of individuals suspected of terrorist acts and surveillance activities, requires prior authorization from a court and is subject to effective, regular and independent oversight […];

Concluding Observations on the Seventh Periodic Report of Germany, Human Rights Committee, UN Doc CCPR/C/DEU/CO/7 (11 November 2021)

42. The Committee is concerned about the wide reaching powers of surveillance, including online surveillance and the hacking of encrypted communications data during criminal investigations. […]

43. The State party should ensure that all types of surveillance activities and interference with privacy are in full conformity with the Covenant, in particular article 17. Such activities should […] be subject to judicial authorisation. […]

Concluding Observations on the Third Periodic Report of Tajikistan, Human Rights Committee, UN Doc CCPR/C/TJK/CO/3 (22 August 2019)

42. The State party should ensure that: […] (b) surveillance and interception is conducted subject to judicial authorization and to effective and independent oversight mechanisms; […]

Concluding Observations on the Third Periodic Report of Lebanon, Human Rights Committee, UN Doc CCPR/C/LBN/CO/3 (9 May 2018)

34. The State party […] should, inter alia, ensure that (a) surveillance, collection of, access to and use of data and communications data are tailored to specific legitimate aims, are limited to a specific number of persons and are subject to judicial authorization; [...]

Concluding Observations on the Fourth Periodic Report of Rwanda, Human Rights Committee, UN Doc CCPR/C/RWA/CO/4 (2 May 2016)

35. The Committee is concerned that Law No 60/2013 permits the interception of communications without prior authorization of a judge.

36. The State party should take legislative and other measures necessary to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity. […] It should also ensure the effectiveness and independence of a monitoring system for such interception, in particular by providing for the judiciary to take part in the authorization and monitoring of the interception.

Concluding Observations on the Sixth Periodic Report of New Zealand, Human Rights Committee, UN Doc CCPR/C/NZL/CO/6 (28 April 2016)

15. The Committee is further concerned about the limited judicial authorization process for the interception of communications of New Zealanders and the total absence of such authorization for the interception of communications of non-New Zealanders.

Concluding Observations on the Initial Report of South Africa, Human Rights Committee, UN Doc CCPR/C/ZAF/CO/1 (27 April 2016)

43. […] The State party should refrain from engaging in mass surveillance of private communications without prior judicial authorization. […]

Concluding Observations on the Fourth Periodic Report of the Republic of Korea, Human Rights Committee, UN Doc CCPR/C/KOR/CO/4 (3 December 2015)

43. The State party should introduce the legal amendments necessary to ensure that any surveillance, including for the purposes of State security, is compatible with the Covenant. It should, inter alia, ensure that subscriber information may be issued with a warrant only.

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/7 (17 August 2015)

24. The State Party should: [...] (c) Ensure that robust oversight systems over surveillance, interception and intelligence-sharing of personal communications activities are in place, including by providing for judicial involvement in the authorization of such measures in all cases, and by considering the establishment of strong and independent oversight mandates with a view to preventing abuses.

Concluding Observations on the Fifth Periodic Report of France, Human Rights Committee, UN Doc CCPR/C/FRA/CO/5 (17 August 2015)

12. [...] It should also ensure the effectiveness and independence of a monitoring system for surveillance activities, in particular by making provision for the judiciary to take part in the authorization and monitoring of surveillance measures.

Concluding Observations on the Sixth Periodic Report of Canada, Human Rights Committee, UN Doc CCPR/C/CAN/CO/6 (13 August 2015)

10. […] The Committee is also concerned about the lack of adequate and effective oversight mechanisms to review activities of security and intelligence agencies and the lack of resources and power of existing mechanisms to monitor such activities [...] The State Party should […] (d) Establish oversight mechanisms over security and intelligence agencies that are effective and adequate and provide them appropriate powers as well as sufficient resources to carry out their mandate; (e) Provide for judicial involvements in the authorization of surveillance measures […]"

Concluding Observations on the Initial Periodic Report of Malawi, Human Rights Committee, UN Doc CCPR/C/MWI/CO/1/Add.1 (19 August 2014)

20. The Committee is concerned that the legal provision expanding the authorization of searches without warrant is still in force [...] The State Party should: (a) Reconsider repealing section 35 of the Police Act in order to prevent arbitrary searches and interference with liberty and privacy."

Commissioner for Human Rights, Council of Europe, Positions on Counter-Terrorism and Human Rights Protection, CommDH/PositionPaper(2015)1 (5 June 2015)

[…] Surveillance activities should be authorised by a judge, set out strict limits on its duration, as well as rules on the disclosure and destruction of surveillance data, and provide for ex post remedies to all individuals concerned."

***Podchasov v Russia*, App No 33696/19, Judgment, European Court of Human Rights (13 February 2024)**

72. […] It observes, however, that in Russia the law-enforcement authorities are not required under domestic law to show the judicial authorisation to the communications service provider before obtaining access to a person's communications. Indeed, pursuant to orders issued by the government, ICOs must install equipment giving the security services direct access to the data stored (see paragraphs 24-26 above). The law-enforcement authorities thus have direct remote access to all Internet communications and related communications data.

73. The Court considers that the requirement to show an authorisation to the communications service provider before obtaining access to a person's communications is an important safeguard against abuse by the law-enforcement authorities, ensuring that proper authorisation is obtained in all cases of secret surveillance. The manner in which the access to the stored data is organised in Russia gives the security services technical means to circumvent the authorisation procedure and to access stored Internet communications and communications data without obtaining prior judicial authorisation. Although the possibility of improper action by a dishonest, negligent or overzealous official can never be completely ruled out whatever the system, the Court considers that a system, such as the Russian one, which enables the secret services to access directly the Internet communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great (see *Roman Zakharov*, cited above, §§ 269-70).

***Potoczká and Adamčo v Slovakia*, App No 7286/16, Judgment, European Court of Human Rights (12 January 2023)**

70. In the present case the applicants complained specifically about the warrant and the issuing court's alleged failure to discharge its responsibility in connection with it. Conversely, they made no specific complaint about the warrant's implementation. However, on the facts, the Court notes that the warrant is intrinsically connected with its implementation, in particular because it was the basic prerequisite for the tapping in question, the tapping did take place, the implementing agency was entitled to rely on the warrant without any room for questioning it, and the applicants' objection to the warrant (namely its lack of justification) in substance inherently extends to its implementation. In these circumstances, it is undoubted that the applicants' complaint relates to an interference with their rights under Article 8 of the Convention to respect for private life and correspondence.

73. The statutory requirement for the phone-tapping warrant to be supported by reasoning is consonant with the Convention case-law, pursuant to which the verification by the authority empowered to authorise the use of secret surveillance that, inter alia, the use of such measures is confined to cases in which there are factual grounds for suspecting a person of planning, committing or having committed certain serious criminal acts and that the measures can only be ordered if there is no prospect of successfully establishing the facts by another method or this would be considerably more difficult, constitutes a guarantee of an appropriate procedure designed to ensure that measures are not ordered haphazardly, irregularly or without due and proper consideration. It is therefore important that the authorising authority should have determined whether there was compelling justification for authorising measures of secret surveillance (see *Dragojević*, cited above, § 94, with further references).

74. The warrant in question has not been made available to the Court. Nevertheless, in the absence of any objection by the Government, the Court takes it as established that the warrant contained no reasoning beyond a reference to the PPS's request and an offhand finding that, in view of that request, obtaining the necessary evidence by other means was ineffective or impossible.

75. The Court also notes that the PPS's request for the warrant was not made available to it either. As to any possibility of the contents of that request making up for the lack of reasoning of the warrant if they were to be read together, the Court notes that no such joint reading had been proposed and the PPS itself concluded that the warrant lacked reasoning and could therefore not be used in evidence (see paragraph 17 above).

76. As the warrant contained no reasoning, it cannot be reviewed in terms of necessity in a democratic society for the purposes of Article 8 §2 of the Convention.

77. The warrant therefore fell short of an essential requirement of national law, a fact which not even the Government have sought to contest.

78. The foregoing considerations are sufficient to enable the Court to conclude that that the interference with the applicants' right to respect for their private life and correspondence was not in accordance with the law.

***Haščak v Slovakia*, Apps Nos 58359/12 and 2 others, Judgment, European Court of Human Rights (23 June 2022)**

92. The Court is likewise aware that, unlike in the case of Mr Varga, in the present case there was no finding by the ordinary courts that the implementation of the warrants by the SIS had violated the applicant's right to the protection of his personal integrity (contrast § 59 of the *Zoltán Varga* judgment). It is, however, of the view that if this factual distinction made any difference at all to the assessment of the present case, it was to the benefit of the applicant. The reasons are twofold.

93. Firstly, the ordinary courts in the case of Mr Varga made no assessment of the actions of the SIS and based their findings – currently subject to an appeal on points of law (see paragraph 40 above) – on the quashing of the warrants by the Constitutional Court (ibid., §§ 154-55). Secondly,

the fact that the outcome of an action brought by Mr Varga that was essentially identical to that brought by the applicant in the instant case has been even less favourable for the applicant than for Mr Varga accentuates the conclusion that the action in question has constituted no effective remedy in the applicant's individual case.

95. The Court finds that the situation in the present case is aggravated by two additional factors. Firstly, while it is accepted that the implementation of the warrant of 2005 interfered with the applicant's right to respect for his privacy, there has been no indication that the warrant actually targeted him. It is accordingly plausible that he was affected in a random manner by its implementation, as he has contended. In that respect, the applicant further argued (and that argument has in no way been refuted by the Government) that the applicable law actually provided no protection to persons randomly affected by covert surveillance measures. Secondly, as appears to be exemplified by the recent controversy between the Prosecutor General and the OSP (see paragraphs 56 and 60 above), there is a protracted fundamental uncertainty in the applicable legal framework as to the practical and procedural status of the presumably leaked primary material from the implementation of the two warrants.

***Ekimdzhiev and Ors v Bulgaria*, App No 70078/12, Judgment, European Court of Human Rights (11 January 2022)**

301. But even if it is accepted that under Bulgarian law the protection of national security can be a standalone ground for secret surveillance, that does not in itself contravene Article 8 of the Convention (see *Association for European Integration and Human Rights and Ekimdzhiev*, 84; *Centrum för rättvisa*, § 261; and *Big Brother Watch and Others*, § 347, all cited above). What rather matters is that any potential abuses flowing from the inherently vague meaning and contours of the notion of national security can be checked. It must be noted in this connection that even when it comes to national security, the relevant authorities must seek judicial authorisation for the surveillance, which can limit their discretion in interpreting that notion and ensure that sufficient reasons to place someone under surveillance are present in each case (see *Roman Zakharov*, cited above, § 249). This is an important safeguard against arbitrariness and abuse. Its effectiveness is analysed in paragraphs 307 to 322 below.

305. Bulgarian law lays down clearly the initial and maximum duration of secret surveillance measures (see paragraph 79 above). It is also clear that surveillance beyond the initially authorised period is only possible if authorised by the competent judge, who must be presented not only with the same information as that required for the initial authorisation, but also with a full account of any surveillance results obtained so far (see paragraph 42 above). Lastly, the law sets out the circumstances in which surveillance must be stopped (see paragraph 82 above). There is, all the same, one area of concern, and that is the potential duration of the initial authorisation for surveillance on national-security grounds, which is up to two years (see paragraph 79 (b) above). The sheer length of that period, coupled with the inherently unclear contours of the notion of national security, significantly weakens the judicial control to which such surveillance must be subjected. […] Even if, as asserted by the Government (see paragraph 286 above), in practice the courts never issue such warrants for periods exceeding six months, that is not based on any statutory limitation.

309. By law, surveillance applications must be duly reasoned and set out both the grounds for the requested surveillance and its intended parameters (see paragraphs 39, 40 and 41 above). An application must, in particular, (a) refer to the circumstances giving cause to suspect that a relevant offence is being prepared or committed or has been committed (including when it comes to national security), (b) set out (except in relation to terrorist offences) the investigative steps already taken and the results of any previous inquiries or investigations, (c) explain (except in relation to terrorist offences) why the requisite intelligence cannot be obtained through other means or why such other means would entail exceptional difficulties, and (d) explain (except in relation to terrorist offences) why the intended duration of the surveillance is necessary (see paragraphs 39 (a), (b), (d) and (f), 40 (a), (b), (e) and (f), and 41 (a) above). All materials on which the application is based must either

be enclosed with it from the outset (for applications made outside criminal proceedings), or made available to the competent judge upon request (for applications made in the course of criminal proceedings) (see paragraph 44 above). When examining the application, the judge must review whether all legal prerequisites are in place and rule by means of a reasoned decision (see paragraph 51 above). One possible shortcoming at that stage is that although surveillance-warrant proceedings must of necessity be conducted without notice to the persons intended to be placed under surveillance, the requesting authority is under no duty to disclose to the judge fully and frankly all matters relevant to the well-foundedness of its surveillance application, including matters which may weaken its case.

310. […] it must also be seen whether those safeguards are being properly applied in practice.

312. As is apparent from two recent judgments of the Specialised Criminal Court, about thirty surveillance warrants issued by its president and vice-presidents had completely blanket contents, were couched in terms which were general enough to be capable of relating to any possible surveillance application, and lacked any reference to the specific case to which they related except the number of the application (see paragraphs 64 and 65 above). There is no reason to think that those warrants were somehow exceptional and represent anything other than the normal practice in that court.

313. It can thus be concluded that no proper reasons have been given for the decisions to issue the vast majority of all surveillance warrants issued in Bulgaria in the past decade. This is of particular relevance as the contemporaneous provision of reasons is a vital safeguard against abusive surveillance (see *Dragojević v. Croatia*, no. 68955/11, §§ 88-101, 15 January 2015; *Dudchenko v. Russia*, no. 37717/05, §§ 97-98, 7 November 2017; and *Liblik and Others v. Estonia*, nos. 173/15 and 5 others, §§ 137-41, 28 May 2019). This is because the provision of reasons, even if succinct, is the only way of ensuring that the judge examining a surveillance application has properly reviewed the application and the materials which support it, and has truly directed his or her mind to the questions whether the surveillance would be a justified and proportionate interference with the Article 8 rights of the person(s) against whom it will be directed, and of any person(s) likely to be collaterally affected by it. In Bulgaria, that is particularly important in view of the applicants' allegation – which seems corroborated by, *inter alia*, some recent developments (see paragraph 67 above) – that criminal proceedings can be opened in a frivolous and abusive manner, chiefly with a view to making it possible to place someone under surveillance for ulterior motives (see paragraph 279 above). As demonstrated by the arrangements in the Sofia City Court since August 2015, the provision of reasons, regardless of whether a surveillance application is allowed or refused, is not unachievable in practice, in spite of the fairly short time-limits for ruling on such applications (see paragraph 60 above).

314. It is true that, as noted in the two above-mentioned judgments of the Specialised Criminal Court (see paragraphs 64 and 65 above), the absence of reasons cannot automatically lead to the conclusion that the judges issuing surveillance warrants have not properly reviewed the applications for them. But three factors raise serious misgivings in that respect.

315. The first such factor is the sheer workload entailed by such applications, which by law can only be dealt with by the presidents or vice-presidents of the respective courts. The National Bureau has repeatedly drawn attention to the inadequate staff and resources placed at the disposal of the Specialised Criminal Court to process properly all surveillance applications submitted to its president and vice-presidents (see paragraph 50 above). The Specialised Criminal Court has itself also drawn attention to the ever-increasing workload entailed by the large volume of surveillance applications submitted to it (see paragraphs 62 and 63 above), and the issue has already been highlighted by the Committee of Ministers in the context of its supervision of *Association for European Integration and Human Rights and Ekimdzhiev* (cited above) (see paragraph 229 (b) above).

316. The second factor is the high percentage of surveillance applications which are being allowed (see the table under paragraph 55 above).

317. The third factor is the express position of the Specialised Criminal Court of Appeal – which has direct supervisory jurisdiction over the Specialised Criminal Court – that a judge dealing with a surveillance application need only check whether the formal requirements to allow it are satisfied, without engaging with the materials in support of the application (see paragraph 66 above).

318. All of the above cannot be dismissed as a mere technicality which does not reflect on the substantive operation of the system of secret surveillance in Bulgaria. There is evidence which tends to suggest that the manner in which the competent judges go about examining surveillance applications has resulted in actual instances of unjustified surveillance. July 2021 the Bulgarian Parliament created an *ad hoc* committee to investigate the possibly unlawful and unjustified use of special means of surveillance with respect to opposition politicians, journalists, and hundreds of participants in the 2020 anti-government protests in Bulgaria, on the basis of warrants issued by that court. Although that committee's report, which was finalised in September 2021, is not yet publicly available, the statements which the Minister of Internal Affairs made in Parliament at the time when the committee was being set up already suggest that the problem with the absence of proper judicial scrutiny has seriously affected the surveillance operations authorised by the Specialised Criminal Court (see paragraph 67 above).

321. It follows that the Court cannot be satisfied that the procedures for authorising secret surveillance, as operating in practice in Bulgaria, effectively guarantee that such surveillance is authorised only when genuinely necessary and proportionate in each case (compare with *Roman Zakharov*, cited above, § 262-63).

322. The additional vetting carried out by the surveillance authorities after the grant of judicial authorisation (see paragraph 73 above) cannot remedy that lack of proper judicial scrutiny, for two reasons. First, that vetting is limited to incompatibility *ratione materiae* or obvious mistakes (ibid.). Secondly, the instances in which that additional safeguard has been triggered are apparently extremely rare (see paragraph 75 above).

400. Bulgarian law lays down safeguards intended to ensure that retained communications data is accessed by the authorities only when that is justified. First, only a limited number of authorities can seek access to that data, within the spheres of their respective competencies (see paragraphs 167 to 169 above). More importantly, such access can be granted only by the competent court president or by a judge to whom that power has been delegated (for access requested outside the framework of already pending criminal proceedings), or by a judge of the competent first-instance court (for access requested by a public prosecutor in the course of criminal proceedings) (see paragraphs 173 to 177 above).

401. Those safeguards nonetheless fall short of the requisite standard of effectiveness in several respects.

402. […] By contrast, access applications made in the course of criminal proceedings, although expected to feature information about the alleged offence in connection with which access is being sought, are not expressly required to explain, in terms, why the data at issue is truly needed – they only have to contain a description of the circumstances underlying the access application, which appears to be an altogether looser requirement (see paragraph 172 above). The law does not therefore make it plain in all situations that access in each individual case can be sought and granted only if the resulting interference with the Article 8 rights of the person(s) concerned would be truly necessary and proportionate.

403. As with the procedure for authorising secret surveillance (see paragraph 309 in fine above), a further possible shortcoming at that stage is that although data-access proceedings must of

necessity be conducted without notice to the persons whose communications data is being sought, the authority seeking access is under no duty to disclose to the judge fully and frankly all matters relevant to the well-foundedness of its access application, including matters which may weaken its case.

404. The law does not require that supporting materials be enclosed with the access application either, which can in many cases prevent the judge who deals with the application from properly checking whether it is well-founded.

405. Nor does the law require judges examining such applications to give reasons explaining why they have decided that granting access to the communications data at issue was truly necessary (see paragraphs 179 and 180 above). As already noted in relation to the procedure for authorising secret surveillance (see paragraph 313 above), the provision of reasons, even if succinct, is the only way of ensuring that the judge examining an access application has properly reviewed the application and the materials which support it, and has truly directed his or her mind to the questions whether accessing the communications data at issue would be a justified and proportionate interference with the Article 8 rights of the person(s) whose data is being accessed, and any person(s) likely to be collaterally affected by that.

406. It follows that the procedures for authorising the authorities to access retained communications data do not effectively guarantee that such access is granted only when genuinely necessary and proportionate in each case.

***Azer Ahmadov v Azerbaijan*, App No 3409/10, Judgment, European Court of Human Rights (22 July 2021)**

65. Under Article 259 of the CCrP, on the basis of a reasoned application by the investigator and relevant submissions by the prosecutor in charge of the preliminary investigation, a domestic court could authorise the interception of telephone conversations if there were sufficient grounds to believe that significant information concerning the criminal case was being sent or received by a suspect or an accused person (see paragraph 33 above). In the instant case, the applicant was neither a suspect nor an accused person; he was never questioned as a witness or participated in the criminal investigation in any other capacity and there was no court decision authorising the tapping of his telephone conversations.

67. […] It is unclear whether Article 259 of the CCrP permitted the interception of the telephone conversations of the victim of an offence under investigation. […]

69. […] While it is not the Court's role to replace the national courts in the establishment of the facts, it cannot but observe that it is difficult to understand how the above undisputed facts could possibly lead to the conclusion that the same telephone number was used by both the applicant and A.K. […].

71. The Court has held that as secret surveillance is a serious interference with a person's right to respect for private life, the judicial authorisation serving as the basis for such surveillance cannot be drafted in such vague terms as to leave room for speculation and assumptions with regard to its content and, most importantly, with regard to the person in respect of whom the measure is being applied […]. In the instant case, in the absence of clarity as to which telephone number or numbers were to be tapped and what was the connection between those numbers and a person genuinely suspected of having committed a criminal offence, the word "contacts" in the decision of 14 March 2008 and the terms of that decision as a whole were too broad and imprecise.

***Zoltán Varga v Slovakia*, App No 58361/12 and 2 others, Judgment, European Court of Human Rights (20 July 2021)**

162. In sum, in view of the lack of clarity of the applicable jurisdictional rules, the lack of procedures for the implementation of the existing rules and flaws in their application, when implementing the three warrants the SIS practically enjoyed a discretion amounting to unfettered power, not being accompanied by a measure of protection against arbitrary interference as required by the rule of law (see paragraph 151 above). Accordingly, it was not "in accordance with the law" for the purposes of Article 8 § 2 of the Convention.

163. In that connection, the Court notes that the question of the efficiency of the judicial supervision in the context of authorising TMGI appears to be of lasting concern irrespective of the enactment and entry into force of the PP Act in 2003 (see *Kvasnica*, cited above, § 20).

***Berlizev v Ukraine*, App No 43571/12, Judgment, European Court of Human Rights (8 July 2021)**

38. It is common ground between the parties that the video-recording of the applicant's conversation with G. constituted an interference with his right to respect for his private life under Article 8 of the Convention. The Court sees no reason to hold otherwise […].

40. […] The Court has endorsed the importance of this safeguard, emphasising that once it is put in place, the judicial authorities should provide relevant and sufficient reasons for their authorisations of covert operations. However, there is no indication that in the present case any such prior judicial approval was ever obtained by the police.

***Big Brother Watch and Others v The United Kingdom*, Apps Nos 58170/13, 62322/14 and 24960/15, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

350. […] the Court considers that the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review. […]

351. […] Nevertheless, bulk interception should be authorised by an independent body; that is, a body which is independent of the executive. […]

352. […] the independent authorising body should be informed of both the purpose of the interception and the bearers or communication routes likely to be intercepted. This would enable the independent authorising body to assess the necessity and proportionality of the bulk interception operation and also to assess whether the selection of bearers is necessary and proportionate to the purposes for which the interception is being conducted.

354. Taking into account the characteristics of bulk interception (see paragraphs 344-345 above), the large number of selectors employed and the inherent need for flexibility in the choice of selectors, which in practice may be expressed as technical combinations of numbers or letters, the Court would accept that the inclusion of all selectors in the authorisation may not be feasible in practice. Nevertheless, given that the choice of selectors and query terms determines which communications will be eligible for examination by an analyst, the authorisation should at the very least identify the types or categories of selectors to be used.

***Centrum för Rättvisa v Sweden*, App No 35252/08, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

265. Turning first to authorisation, the Grand Chamber considers that while judicial authorisation is an "important safeguard against arbitrariness" it is not a "necessary requirement". Nevertheless, bulk

interception should be authorised by an independent body; that is, a body which is independent of the executive.

266. Furthermore, in order to provide an effective safeguard against abuse, the independent authorising body should be informed of both the purpose of the interception and the bearers or communication routes likely to be intercepted. This would enable the independent authorising body to assess the necessity and proportionality of the bulk interception operation and also to assess whether the selection of bearers is necessary and proportionate to the purposes for which the interception is being conducted.

268. Taking into account the characteristics of bulk interception (see paragraphs 258 and 259 above), the large number of selectors employed and the inherent need for flexibility in the choice of selectors, which in practice may be expressed as technical combinations of numbers or letters, the Court would accept that the inclusion of all selectors in the authorisation may not be feasible in practice. Nevertheless, given that the choice of selectors and query terms determines which communications will be eligible for examination by an analyst, the authorisation should at the very least identify the types or categories of selectors to be used."

302. However, for the purposes of the Court's analysis, at this stage the relevant point is that the Swedish authorisation system offers a judicial ex ante review of permit requests which is comprehensive, in the sense that the aim of the mission and the bearers and categories of selectors to be used are subject to control, and is sufficiently detailed in respect of secret bulk signals intelligence as part of foreign intelligence. Such a review offers a significant safeguard against, notably, the launch of abusive or clearly disproportionate bulk interception operations. Importantly, it also sets the framework within which a concrete operation must unfold and the limits whose observance then becomes the object of the applicable supervision and ex post facto control mechanisms.

***Hambardzumyan v Armenia*, App No 43478/11, Judgment, European Court of Human Rights (5 December 2019)**

65. […] secret surveillance being a serious interference with a person's right to respect for private life, a judicial authorisation serving as its basis cannot be drafted in such vague terms as to leave room for speculation and assumptions with regard to its content and, most importantly, to the person in whose respect the given measure is being applied.

***Liblik and Others v Estonia*, Apps Nos 173/15 and 5 others, Judgment, European Court of Human Rights (28 May 2019)**

129. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see *Roman Zakharov*, cited above, § 230).

137. Despite the requirement that authorisations had to contain reasons as to the statutory conditions concerning reasonable suspicion and the *ultima ratio* principle being satisfied, in the applicants' case, the decisions issued by the preliminary investigation judges included only superficial and declaratory statements, whereas the prosecutors' authorisations did not contain any reasoning […].

140. […] It was exactly this practice of circumventing the requirement to provide reasons at the initial authorisation stage and accepting that they could also be provided later during the proceedings which opened a door to arbitrariness contrary to the guarantees under Article 8 of the Convention.

[…]

141. With respect to the practice of accepting retrospectively provided reasoning, the Court notes that the effectiveness of the safeguard of prior scrutiny and obligation to provide reasons may not be the same where the obligation of prior scrutiny and provision of reasons is replaced with the possibility to provide such reasons later at the trial stage, where the courts inevitably have more information about how the alleged offences were committed. It is not merely the lapse of time, but the different procedural context in which such reasons would be provided, which calls for such caution.

142. In the light of the reasons set out above, the Court finds that as the interferences with the applicants' private life and correspondence did not comply with the requirement under domestic law that authorisations of secret surveillance be duly reasoned, those interferences were not "in accordance with the law" as required by Article 8 § 2 of the Convention.

***Konstantin Moskalev v Russia*, App No 59589/10, Judgment, European Court of Human Rights (7 November 2017)**

51. […], although Russian law requires that a judge be immediately informed of each instance of urgent interception, his or her power is limited to authorising the extension of the interception measure beyond forty-eight hours. He or she has no power to assess whether the use of the urgent procedure was justified or to decide whether the material obtained during the previous forty-eight hours is to be kept or destroyed.

52. The Court considers that the defects of the "urgent procedure" identified in *Roman Zakharov* fully appeared in the present case. Indeed, although a judge was notified about the urgent interception of the applicant's telephone communications, she did not carry out any judicial review of the police's decision to tap the applicant's telephone. No authority independent of the authorities carrying out the interception assessed whether the use of the urgent procedure had been justified, whether the police's decision had been based on a reasonable suspicion that the applicant had committed a criminal offence, whether the interception had been "necessary in a democratic society" and, in particular, whether it had been proportionate to any legitimate aim pursued. The interception of the applicant's communications by means of the "urgent procedure" was not therefore attended by appropriate safeguards against arbitrariness.

***Szabó and Vissy v Hungary*, App No 37138/14, Judgment, European Court of Human Rights (12 January 2016)**

73. [...] Moreover, particularly in this context the Court notes the absence of prior judicial authorisation for interceptions ... This safeguard would serve to limit the law-enforcement authorities' discretion in interpreting the broad terms of "persons concerned identified ... as a range of persons" by following an established judicial interpretation of the terms or an established practice to verify whether sufficient reasons for intercepting a specific individual's communications exist in each case. It is only in this way that the need for safeguards to ensure that emergency measures are used sparingly and only in duly justified cases can be satisfied. [...]

80. The Court concedes that by the nature of contemporary terrorist threats there can be situations of emergency in which the mandatory application of judicial authorisation is not feasible, would be counterproductive for lack of special knowledge or would simply amount to wasting precious time. This is especially true in the present-day upheaval caused by terrorist attacks experienced throughout the world and in Europe, all too often involving important losses of life, producing numerous casualties and significant material damage, which inevitably disseminate a feeling of insecurity amongst citizens. [...]

81. Furthermore, where situations of extreme urgency are concerned, the law contains a provision

under which the director of the service may himself authorise secret surveillance measures for a maximum of 72 hours. For the Court, this exceptional power should be sufficient to address any situations in which external, judicial control would run the risk of losing precious time. Such measures must however be subject to a post factum review, which is required, as a rule, in cases where the surveillance was authorised ex ante by a non-judicial authority.

***Roman Zakharov v Russia*, App No 47143/06, Judgment, European Court of Human Rights (4 December 2015)**

249. the Court does not lose sight of the fact that prior judicial authorisation for interceptions is required in Russia. Such judicial authorisation may serve to limit the law-enforcement authorities' discretion in interpreting the broad terms of "a person who may have information about a criminal offence", "a person who may have information relevant to the criminal case", and "events or activities endangering Russia's national, military, economic or ecological security" by following an established judicial interpretation of the terms or an established practice to verify whether sufficient reasons for intercepting a specific individual's communications exist in each case. The Court accepts that the requirement of prior judicial authorisation constitutes an important safeguard against arbitrariness. The effectiveness of that safeguard will be examined below.

250. The Court has held that it is not unreasonable to leave the overall duration of interception to the discretion of the relevant domestic authorities which have competence to issue and renew interception warrants, provided that adequate safeguards exist, such as a clear indication in the domestic law of the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled. […]

261. The Court notes that in Russia judicial scrutiny is limited in scope. Thus, materials containing information about undercover agents or police informers or about the organisation and tactics of operational-search measures may not be submitted to the judge and are therefore excluded from the court's scope of review. The Court considers that the failure to disclose the relevant information to the courts deprives them of the power to assess whether there is a sufficient factual basis to suspect the person in respect of whom operational-search measures are requested of a criminal offence or of activities endangering national, military, economic or ecological security. The Court has earlier found that there are techniques that can be employed which both accommodate legitimate security concerns about the nature and sources of intelligence information and yet accord the individual a substantial measure of procedural justice.

262. Furthermore, the Court observes that in Russia the judges are not instructed, either by the CCrP or by the OSAA, to verify the existence of a "reasonable suspicion" against the person concerned or to apply the "necessity" and "proportionality" test". At the same time [...] The Constitutional Court has therefore recommended, in substance, that when examining interception authorisation requests Russian courts should verify the existence of a reasonable suspicion against the person concerned and should authorise interception only if it meets the requirements of necessity and proportionality.

263. However, the Court observes that the domestic law does not explicitly require the courts of general jurisdiction to follow the Constitutional Court's opinion as to how a legislative provision should be interpreted if such opinion has been expressed in a decision rather than a Judgment. Indeed, the materials submitted by the applicant show that the domestic courts do not always follow the above-mentioned recommendations of the Constitutional Court, all of which were contained in decisions rather than in Judgments. Thus, it transpires from the analytical notes issued by District Courts that interception requests are often not accompanied by any supporting materials, that the judges of these District Courts never request the interception agency to submit such materials and that a mere reference to the existence of information about a criminal offence or activities endangering national, military, economic or ecological security is considered to be sufficient for the authorisation to be granted. An interception request is rejected only if it is not signed by a competent person, contains no reference to the offence in connection with which interception is to be ordered,

or concerns a criminal offence in respect of which interception is not permitted under domestic law. Thus, the analytical notes issued by District Courts, taken together with the statistical information for the period from 2009 to 2013 provided by the applicant, indicate that in their everyday practice Russian courts do not verify whether there is a "reasonable suspicion" against the person concerned and do not apply the "necessity" and "proportionality" test.

264. Lastly, as regards the content of the interception authorisation, it must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information.

265. The Court observes that the CCrP requires that a request for interception authorisation must clearly mention a specific person whose communications are to be intercepted, as well as the duration of the interception measure. By contrast, the OSAA does not contain any requirements either with regard to the content of the request for interception or to the content of the interception authorisation. As a result, courts sometimes grant interception authorisations which do not mention a specific person or telephone number to be tapped, but authorise interception of all telephone communications in the area where a criminal offence has been committed. Some authorisations do not mention the duration for which interception is authorised. The Court considers that such authorisations, which are not clearly prohibited by the OSAA, grant a very wide discretion to the law-enforcement authorities as to which communications to intercept, and for how long.

266. The Court further notes that in cases of urgency it is possible to intercept communications without prior judicial authorisation for up to forty-eight hours. A judge must be informed of any such case within twenty-four hours from the commencement of the interception. If no judicial authorisation has been issued within forty-eight hours, the interception must be stopped immediately. The Court has already examined the "urgency" procedure provided for in Bulgarian law and found that it was compatible with the Convention. However, in contrast to the Bulgarian provision, the Russian "urgent procedure" does not provide for sufficient safeguards to ensure that it is used sparingly and only in duly justified cases [...] The domestic law does not limit the use of the urgency procedure to cases involving an immediate serious danger to national, military, economic or ecological security. It leaves the authorities an unlimited degree of discretion in determining in which situations it is justified to use the non- judicial urgent procedure, thereby creating possibilities for abusive recourse to it. Furthermore, although Russian law requires that a judge be immediately informed of each instance of urgent interception, his or her power is limited to authorising the extension of the interception measure beyond forty-eight hours. He or she has no power to assess whether the use of the urgent procedure was justified or to decide whether the material obtained during the previous forty-eight hours is to be kept or destroyed. Russian law does therefore not provide for an effective judicial review of the urgency procedure.

267. In view of the above considerations the Court considers that the authorisation procedures provided for by Russian law are not capable of ensuring that secret surveillance measures are not ordered haphazardly, irregularly or without due and proper consideration.

268. The Court takes note of the applicant's argument that the security services and the police have the technical means to intercept mobile telephone communications without obtaining judicial authorisation, as they have direct access to all communications and as their ability to intercept the communications of a particular individual or individuals is not conditional on providing an interception authorisation to the communications service provider.

269. The Court considers that the requirement to show an interception authorisation to the communications service provider before obtaining access to a person's communications is one of the important safeguards against abuse by the law-enforcement authorities, ensuring that proper authorisation is obtained in all cases of interception [...] in particular the addendums to Order No70, communications service providers must install equipment giving the law- enforcement authorities

direct access to all mobile telephone communications of all users. The communications service providers also have an obligation under Order no 538 to create databases storing information about all subscribers, and the services provided to them, for three years; the secret services have direct remote access to those databases. The law-enforcement authorities thus have direct access to all mobile telephone communications and related communications data.

270. The Court considers that the manner in which the system of secret surveillance operates in Russia gives the security services and the police technical means to circumvent the authorisation procedure and to intercept any communications without obtaining prior judicial authorisation. Although the possibility of improper action by a dishonest, negligent or over- zealous official can never be completely ruled out whatever the system, the Court considers that a system, such as the Russian one, which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great.

***Iordachi and Others v Moldova*, App No 25198/02, Judgment, European Court of Human Rights (10 February 2009)**

40. Moreover, the Court recalls that in *Dumitru Popescu v. Romania* the Court expressed the view that the body issuing authorisations for interception should be independent and that there must be either judicial control or control by an independent body over the issuing body's activity [...]

47. […], it would appear that the investigating judge plays a very limited role. According to Article 41 of the Code of Criminal Procedure, his role is to issue interception warrants. According to Article 136 of the same Code, the investigating judge is also entitled to store "the original copies of the tapes along with the complete written transcript in a special place in a sealed envelope" and to adopt "a decision regarding the destruction of records which are not important for the criminal case". However, the law makes no provision for acquainting the investigating judge with the results of the surveillance and does not require him or her to review whether the requirements of the law have been complied with. On the contrary, section 19 of the Law on Operational Investigative Activities appears to place such supervision duties on the "Prosecutor General, his or her deputy, and the municipal and county prosecutors". […]

48. Another point which deserves to be mentioned in this connection is the apparent lack of regulations specifying with an appropriate degree of precision the manner of screening the intelligence obtained through surveillance, or the procedures for preserving its integrity and confidentiality and the procedures for its destruction.

49. The Court further notes that overall control of the system of secret surveillance is entrusted to the Parliament which exercises it through a specialised commission. However, the manner in which the Parliament effects its control is not set out in the law and the Court has not been presented with any evidence indicating that there is a procedure in place which governs the Parliament's activity in this connection. […]

51. The Court notes further that in 2007 the Moldovan courts authorised virtually all the requests for interception made by the prosecuting authorities. Since this is an uncommonly high number of authorisations, the Court considers it necessary to stress that telephone tapping is a very serious interference with a person's rights and that only very serious reasons based on a reasonable suspicion that the person is involved in serious criminal activity should be taken as a basis for authorising it. The Court notes that the Moldovan legislation does not elaborate on the degree of reasonableness of the suspicion against a person for the purpose of authorising an interception. Nor does it contain safeguards other than the one provided for in section 6(1), namely that interception should take place only when it is otherwise impossible to achieve the aims. This, in the Court's

opinion, is a matter of concern when looked at against the very high percentage of authorisations issued by investigating judges. For the Court, this could reasonably be taken to indicate that the investigating judges do not address themselves to the existence of compelling justification for authorising measures of secret surveillance.

52. In this connection, the Court notes the statistical information contained in the letter of the Head of the President's Office of the Supreme Court of Justice. According to that information, in 2005 over 2,500 interception warrants were issued, in 2006 some 1,900 were issued and over 2,300 warrants were issued in 2007. These figures show that the system of secret surveillance in Moldova is, to say the least, overused, which may in part be due to the inadequacy of the safeguards contained in the law.

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet OEA/Ser.L/V/II. CIDH/RELE/INF.11/13 (31 December 2013)

164. […] the Special Rapporteurs have already underscored the need for effective controls to ensure that online surveillance programs are designed and implemented taking account of all of the rights at stake, including the procedural guarantees.

165. In light of the above, decisions to undertake surveillance activities that invade the privacy of individuals must be authorized by independent judicial authorities, who must state why the measure is appropriate for the accomplishment of the objectives pursued in the specific case; whether it is sufficiently restricted so as not to infringe upon the right in question more than necessary; and whether it is proportionate in relation to the interests pursued. In this respect, the European Court of Human Rights has held that "in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge." States must ensure that the judicial authority is specialized and competent to make decisions on the legality of the communications surveillance, the technologies used, and its impact on the sphere of rights that could be involved.

***Garcia v Peru*, Inter-American Court of Human Rights, Case 11.006, Report No 1/95, OEA/Ser.L/V/II.88, The Merits (17 February 1995)**

The guarantee of the inviolability of the domicile and of private papers must give way when there is a well-substantiated search warrant issued by a competent judicial authority, spelling out the reasons for the measure being adopted and specifying the place to be searched and the objects that will be seized.

The 1979 Constitution of Peru stipulated the inviolability of domicile and of private papers except when an order has been issued by a competent judicial authority authorizing the search, explaining its reasons and, where appropriate, authorizing the seizure of private papers, while respecting the guarantees stipulated by law.

Based on these concepts, the Commission concludes that the warrantless search of Dr. García's home and the seizure of private family papers - actions committed by Peruvian Army soldiers - were committed in complete disregard of the procedural requirements stipulated in the Constitution. The violation of those requirements indicates that the Government of Peru failed to guarantee to Dr. Alan García and to his family the full exercise of their right to privacy.

***Ligue des droits humains v Conseil des ministres* (C-817/19), Judgment, Grand Chamber, Court of Justice of the European Union (21 June 2022)**

223. In particular, in order to ensure, in practice, that fundamental rights are fully observed in the system put in place by the PNR Directive and, in particular, the conditions set out in paragraphs 218

and 219 above, it is essential that disclosure of PNR data for the purposes of subsequent assessment be, as a general rule, except in the event of duly justified urgency, subject to a prior review carried out either by a court or by an independent administrative authority, and that the decision of that court or body be made following a reasoned request by the competent authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime. In the event of duly justified urgency, the review must take place within a short time (see, by analogy, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 202and the case-law cited, and judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 110).

224. In those circumstances, the requirement for prior review under Article 12(3)(b) of the PNR Directive, for requests for the disclosure of PNR data introduced after the expiry of a period of six months following the transfer of those data to the PIU must also apply, mutatis mutandis, where the request for disclosure is introduced before the expiry of that period.

***G.D. v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, and Attorney General*, (C-140/20), Judgment, Grand Chamber, Court of Justice of the European Union (5 April 2022)**

106. In order to ensure, in practice, that those conditions are fully observed, it is essential that access by the competent national authorities to retained data be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime (judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 51 and the case-law cited).

107 One of the requirements for the prior review is that the court or independent administrative body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that court or body must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access (judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 52).

108. Where that review is carried out not by a court but by an independent administrative body, that body must have a status that enables it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence. Accordingly, it follows that the requirement of independence that has to be satisfied by the body entrusted with carrying out the prior review means that that body must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially and free from any external influence. In particular, in the criminal field the requirement of independence entails that the body entrusted with the prior review, first, should not be involved in the conduct of the criminal investigation in question and, second, must have a neutral stance vis-à-vis the parties to the criminal proceedings (see, to that effect, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraphs 53 and 54).

109. Thus, the Court has, inter alia, found that a public prosecutor's office, which directs the investigation procedure and, where appropriate, brings the public prosecution cannot be considered to have third party status in relation to the interests at issue, since it has the task not of ruling on a case in complete independence but, acting as prosecutor in the proceedings, of bringing it, where appropriate, before the court that has jurisdiction. Consequently, a public prosecutor's office is not

in a position to carry out the prior review of requests for access to retained data (see, to that effect, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications),* C-746/18, EU:C:2021:152, paragraphs 55 and 57).

110. Finally, the independent review required in accordance with Article 15(1) of Directive 2002/58 must take place before any access to the data concerned, except in the event of duly justified urgency, in which case the review must take place within a short time. A subsequent review would not enable the objective of a prior review, consisting in preventing the authorisation of access to the data in question that exceeds what is strictly necessary, to be met (see, to that effect, judgments of 6 October 2020, La *Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 189, and of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 58).

111. In the present case, it is apparent from the order for reference that the 2011 Act assigns to a police officer, whose rank is not below that of chief superintendent, the power to carry out the prior review of requests for access to data issued by the police investigation services and to request the providers of electronic communications services to transmit the data that they retain to those services. To the extent that that officer does not have the status of a third party in relation to those services, he or she does not fulfil the requirements for independence and impartiality recalled in paragraph 108 of this judgment, notwithstanding the fact that he or she is assisted in that duty by a police unit, in this case the TLU, which benefits from a certain degree of autonomy in the exercise of its duties.

112. Next, while it is true that the 2011 Act provides for mechanisms of review subsequent to the decision of the competent police officer in the form of a complaint procedure and a procedure before a judge responsible for examining the application of the provisions of that act, it is clear from the case-law recalled in paragraph 110 of this judgment that a review carried out subsequently cannot be substituted for the requirement, recalled in paragraph 106 of this judgment, for a review that is independent and, except in duly justified urgent cases, undertaken beforehand.

113. Finally, the 2011 Act does not lay down any objective criteria which define precisely the conditions and circumstances in which national authorities must be granted access to data and the police officer responsible for processing the requests for access to retained data is solely competent, as Ireland confirmed at the hearing, to assess the suspicions that exist with respect to the persons concerned and the need for access to data that relate to them.

114. Consequently, the answer to the third question is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation pursuant to which the centralised processing of requests for access to data retained by providers of electronic communications services, issued by the police in the context of the investigation or prosecution of serious criminal offences, is the responsibility of a police officer, who is assisted by a unit established within the police service which has a degree of autonomy in the exercise of its duties, and whose decisions may subsequently be subject to judicial review.

***La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées; Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministers* (C-511/18, C-512/18 and C-520/18), Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2020)**

189. In addition, a decision authorising the real-time collection of traffic and location data must be based on objective criteria provided for in the national legislation. In particular, that legislation must define, in accordance with the case-law cited in paragraph 176 of the present judgment, the circumstances and conditions under which such collection may be authorised and must provide that,

as was pointed out in the previous paragraph, only persons with a link to the objective of preventing terrorism may be subject to such collection. In addition, a decision authorising the real-time collection of traffic and location data must be based on objective and non-discriminatory criteria provided for in national legislation. In order to ensure, in practice, that those conditions are observed, it is essential that the implementation of the measure authorising real-time collection be subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding, with that court or body having to satisfy itself, inter alia, that such real-time collection is authorised only within the limits of what is strictly necessary […]. In cases of duly justified urgency, the review must take place within a short time.

192. […] recourse to the real-time collection of traffic and location data is limited to persons in respect of whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities and is subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding in order to ensure that such real-time collection is authorised only within the limits of what is strictly necessary. In cases of duly justified urgency, the review must take place within a short time.

III. EFFECTIVE OVERSIGHT

The review of pronouncements by different human rights monitoring mechanisms shows that there are significant overlaps in references to the requirements of judicial authorization and effective oversight. It may therefore be pertinent to consult both sub-chapters. Reference to the requirement of effective oversight within the broader framework of adequate safeguards accompanying surveillance can be found in the introductory sub-chapter E.

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

7. *Calls upon* all States: (e) To establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data;

** See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014)*

UN Human Rights Council Resolution on New and Emerging Digital Technologies and Human Rights, UN Doc A/HRC/RES/53/29 (14 July 2023)

3. *Highlights* the importance of the need to respect, protect and promote human rights and fundamental freedoms, in recognition of the inherent dignity of the human person, throughout the lifecycle of artificial intelligence systems and, towards this end, the need to pay particular attention to: (e) Strengthening, as necessary, the oversight and enforcement capacity of respective States relevant to artificial intelligence and sectors where artificial intelligence is being applied to allow more effective measures to protect against human rights risks relating to artificial intelligence;

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

40. Oversight frameworks may integrate a combination of administrative, judicial and/or parliamentary oversight. Oversight bodies should be independent of the authorities carrying out the surveillance and equipped with appropriate and adequate expertise, competencies and resources. Authorization and oversight should be institutionally separated. Independent oversight bodies should proactively investigate and monitor the activities of those who conduct surveillance and have access to the products of surveillance, and carry out periodic reviews of surveillance capabilities and technological developments. The agencies carrying out surveillance should be required to provide all the information necessary for effective oversight upon request and regularly report to the oversight bodies, and they should be required to keep records of all surveillance measures taken. Oversight processes must also be transparent and subject to appropriate public scrutiny and the decisions of the oversight bodies must be subject to appeal or independent review. Exposing oversight bodies to divergent points of view, for example through expert and multi-stakeholder consultations (see for example A/HRC/34/60, para. 36), is

particularly important in the absence of an adversarial process: it is essential that "points of friction" — continual challenges to approaches and understandings — be built in.

***Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, App No 62540/00, Judgment, European Court of Human Rights (28 June 2007)**

77. In addition, in the context of secret measures of surveillance by public authorities, because of the lack of public scrutiny and the risk of misuse of power, the domestic law must provide some protection against arbitrary interference with Article 8 rights (see *Klass and Others*, cited above, pp. 25-26, §§ 54-56; mutatis mutandis, *Leander v. Sweden*, judgment of 26 March 1987, Series A no. 116, pp. 25-27, §§ 60-67; *Halford*, cited above, p. 1017, § 49; *Kopp*, cited above, p. 541, § 64; and *Weber and Saravia*, cited above, § 94). The Court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law (see *Klass and Others*, cited above, p. 23, § 50).

85. Unlike the system of secret surveillance under consideration in the case of *Klass and Others*, the SSMA does not provide for any review of the implementation of secret surveillance measures by a body or official that is either external to the services deploying the means of surveillance or at least required to have certain qualifications ensuring his independence and adherence to the rule of law. Under the SSMA, no one outside the services actually deploying special means of surveillance verifies such matters as whether these services in fact comply with the warrants authorising the use of such means, or whether they faithfully reproduce the original data in the written record. Similarly, there exists no independent review of whether the original data is in fact destroyed within the legal ten-day time-limit if the surveillance has proved fruitless. On the contrary, it seems that all these activities are carried out solely by officers of the Ministry of Internal Affairs. It is true that the Code of 1974 provided, in its Article 111b § 6, that the judge who had issued a surveillance warrant had to be informed when the use of special means of surveillance has ended. So does Article 175 § 6 of the Code of 2005. It is also true that there is an obligation under section 19 of the SSMA to inform the issuing judge when the use of special means of surveillance has been discontinued before the end of the authorised period. However, the texts make no provision for acquainting the judge with the results of the surveillance and do not command him or her to review whether the requirements of the law have been complied with. Moreover, it appears that the provisions of the Codes of 1974 and 2005 are applicable only in the context of pending criminal proceedings and do not cover all situations envisaged by the SSMA, such as the use of special means of surveillance to protect national security [...]

87. The Court further notes that the overall control over the system of secret surveillance is entrusted solely to the Minister of Internal Affairs – who not only is a political appointee and a member of the executive, but is directly involved in the commissioning of special means of surveillance –, not to independent bodies, such as a special board elected by the Parliament and an independent commission, as was the case in *Klass and Others*, or a special commissioner holding or qualified to hold high judicial office, as was the case in Christie, or a control committee consisting of persons having qualifications equivalent to those of a Supreme Court judge, as was the case in L. v. Norway. A dissenting judge in the Constitutional Court had serious misgivings about this complete lack of external control.

88. Moreover, the manner in which the Minister effects this control is not set out in the law. Neither the SSMA, nor any other statute lays down a procedure governing the Minister's actions in this respect. The Minister has not issued any publicly available regulations or instructions on the subject. Moreover, neither the Minister, nor any other official is required to regularly report to an independent body or to the general public on the overall operation of the system or on the

measures applied in individual cases.

UN General Assembly Resolution on the United Nations Global Counter-Terrorism Strategy: Seventh Review, UN Doc A/RES/75/291 (30 June 2021)

106. *Urges* all States to respect and protect the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, including in the context of digital communication, also while countering terrorism, in accordance with international law, in particular international human rights law, and to take measures to ensure that interferences with or restrictions on that right are not arbitrary or unlawful and are subject to effective oversight and to appropriate redress, including through judicial review or other legal means;

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019)

6. *Calls upon* all States: (e) To establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data;

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

52. […] If used at all, such technologies should only be deployed to respond to situations such as serious crime and serious public safety threats, if discriminatory effects can be excluded and subjected to adequate and effective oversight, including independent authorization and regular independent human rights audits.

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

38. Judicial involvement that meets international standards relating to independence, impartiality and transparency can help to make it more likely that the overall statutory regime will meet the minimum standards that international human rights law requires. At the same time, judicial involvement in oversight should not be viewed as a panacea; in several countries, judicial warranting or review of the digital surveillance activities of intelligence and/or law enforcement agencies have amounted effectively to an exercise in rubber-stamping. Attention is therefore turning increasingly towards mixed models of administrative, judicial and parliamentary oversight... Jurisprudence at the regional level has emphasized the utility of an entirely independent oversight body, particularly to monitor the execution of approved surveillance measures. In 2009, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism suggested, therefore, that "there must be no secret surveillance system that is not under review of an independent oversight body and all interferences must be authorized through an independent body."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights while Counter-Terrorism, Human Rights Implications of the Development, Use, Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism, UN Doc A/HRC/52/39 (1 March 2023)

50. Finally, she highlights the necessity of independent oversight for surveillance and data collection premised on national security or counter-terrorism grounds. Noting that intelligence agencies are driving and adapting technological change and deploying an avalanche of new technologies,

including machine learning, for automated offensive and defence computer network operations, the Special Rapporteur calls for substantial State investment in intelligence oversight capacity. Austerity in surveillance oversight cannot be justified given the evolution of surveillance technology, as the legitimacy of executive conduct depends on effective, modern and comprehensive intelligence oversight. She urges that, as a general practice, oversight bodies be given direct access to the operational systems of intelligence services and that they be allowed to monitor stored data for filer errors. They should also be involved in data minimization verifications. This will ensure oversight of intelligence audit trails and create methods to enable oversight if systematic pattern identification shows high overlap with illegal and inappropriate intelligence database use. […]

56. The Special Rapporteur recommends that States: (d) Establish and support adequately resourced and independent oversight of new technologies in counter-terrorism and security contexts. This includes the establishment of independent data privacy oversight bodies. In parallel, States must ensure that intelligence oversight bodies are adequately resourced and technologically proficient to address the expansive use of technology by intelligence entities. This includes direct access to intelligence services' operational systems, access to stored data, oversight of intelligence audit trails, as well as the establishment of mechanisms of oversight for intelligence cooperation, as set out in the present report;

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 'Reinforcing media freedom and the safety of journalists in the digital age', UN Doc A/HRC/50/29 (20 April 2022)

123. States should incorporate adequate safeguards in national laws, such as judicial oversight, to ensure that digital surveillance laws and activities do not undermine international standards on the protection of journalists and their sources. They should hold surveillance companies accountable for foreseeable use of their technology by their clients to target journalists, and amend sovereign immunity laws to permit civil action against States engaged in cross-border digital attacks on journalists.

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/40/63 (16 October 2019)

46. The Special Rapporteur recommends: (iii) The establishment of one or more independent oversight authorities empowered by law and adequately resourced by the State in order to carry out effective review of any privacy-intrusive activities carried out by intelligence services and law-enforcement agencies; […]

47. The incorporation by UN Member States into their domestic legal system of the standards and safeguards set out in Convention 108+ Article 11, for the protection of the fundamental right to privacy, especially: (c) the establishment of one or more independent oversight authorities empowered by law and adequately resourced by the State in order to carry out effective review of any privacy-intrusive activities carried out by intelligence services and law-enforcement agencies.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

52. Judicial authorization of government use of surveillance technologies is necessary but insufficient. The purchase of these technologies should also be subject to meaningful public oversight, consultation and control. In recent years, as the use of surveillance technologies has proliferated among law enforcement bodies in the United States, several communities have instituted civilian control boards to regulate their use and purchase. The city of Oakland in California, for instance, adopted an ordinance with several features regarding the purchase of surveillance technology that could be replicated by States. These include:

(a) An approval process, carried out by the relevant departments, that takes into account the State's human rights obligations;

(b) Public notice of such purchases through regular processes, and public consultations on issues such as the human rights implications of such purchases and whether the technologies at issue will be effective at achieving their intended purposes;

(c) Regular public reporting on such approvals, purchases and uses.

53. Particularly in States that allow subnational organs a certain autonomy in the purchase of law enforcement tools, community control of such purchases should be encouraged and enforced. Given the clear public interest in maintaining the privacy and security of widely available commercial software, public oversight mechanisms should also be empowered to set policies on the stockpiling of vulnerabilities and the development of relevant exploits."

66. For States: (c) Purchasing States should also establish mechanisms that ensure public or community approval, oversight and control of the purchase of surveillance technologies;

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/23/40 (17 April 2013)

76. […] States should exercise adequate oversight in order to meet their international human rights obligations when they contract with, or legislate for, corporate actors where there may be an impact upon the enjoyment of human rights. Human rights obligations in this regard apply when corporate actors are operating abroad.

93. States should establish independent oversight mechanisms capable to ensure transparency and accountability of State surveillance communications.

Concluding Observations on the Fifth Periodic Report of the Republic of Korea, Human Rights Committee, UN Doc CCPR/C/KOR/CO/5 (30 October 2023)

22. […] It should guarantee independent and effective oversight of law enforcement and security forces in the context of counter-terrorism investigations and surveillance, including timely judicial supervision and review.

Concluding Observations on the Fourth Periodic Report of the Islamic Republic of Iran, Human Rights Committee, UN Doc CCPR/C/IRN/CO/4 (26 October 2023)

46. […] The State party should establish independent oversight mechanisms, including independent and impartial judicial review of surveillance activity, […].

Concluding Observations on the Eighth Periodic Report of Colombia, UN Doc CCPR/C/COL/CO/8 (21 July 2023)

31. […] The State party should also ensure that the processing and collection of personal data are transparent and subject to effective independent oversight mechanisms […].

Concluding Observations on the Second Periodic Report of Lesotho, UN Doc CCPR/C/LSO/CO/2 (21 July 2023)

50. The State party should: (a) Provide adequate human and financial resources for the operationalization of the Data Protection Commission so that it can effectively ensure the protection of the right to privacy in an independent manner;

Concluding Observations on the Initial Report of the State of Palestine, UN Doc CCPR/C/PSE/CO/1 (21 July 2023)

37. […] The Committee is particularly concerned about reports that the Preventive Security Service, which conducts electronic surveillance, is granted extensive monitoring powers, and that the existing oversight mechanism over its activities is not effective (art. 17).

38. In the light of the Committee's general comment No. 16 (1988) on right to privacy, the State party should: (a) Ensure that any interference with the right to privacy, including activities carried out by the Preventive Security Service under Decree-Law No. 10 of 2018 regarding cybercrime, is subject to judicial review and to effective and independent oversight mechanisms;

Concluding Observations on the Fourth Periodic Report of Zambia, Human Rights Committee, UN Doc CCPR/C/ZMB/CO/4 (20 March 2023)

32. […] The State party should also ensure that surveillance activities are subject to effective judicial oversight mechanisms and ensure access to effective remedies in cases of abuse.

Concluding Observations on the Third Periodic Report of Turkmenistan, UN Doc CCPR/C/TKM/CO/3 (17 March 2023)

39. […] the Committee urges the State party to: (b) Guarantee the independent and impartial judicial review of surveillance;

Concluding Observations on the Seventh Periodic Report of Japan, Human Rights Committee, UN Doc CCPR/C/JPN/CO/7 (28 October 2022)

35. […] It should ensure that any interference with the right to privacy requires prior authorization by a court and is subject to effective and independent oversight mechanisms, […]

Concluding Observations on the Fifth Periodic Report of the Philippines, Human Rights Committee, UN Doc CCPR/C/PHL/CO/5 (28 October 2022)

14. The State party should: (d) Ensure that any interference with the right to privacy, including through the publication of the personal data of individuals suspected of terrorist acts and surveillance activities […] is subject to effective, regular and independent oversight […]

Concluding Observations on the Fourth Periodic Report of Hong Kong, China, Human Rights Committee, UN Doc CCPR/C/CHN-HKG/CO/4 (22 July 2022)

40. Hong Kong, China, should: (c) Strengthen the capacity, mandate and powers of the Office of the Privacy Commissioner for Personal Data to carry out independent and effective oversight of surveillance activities and interference with privacy […]

Concluding Observations on the Fifth Periodic Report of Ireland, Human Rights Committee, UN Doc CCPR/C/IRL/CO/5 (22 July 2022)

46. […] The State party should also ensure that the processing and collection of personal data are subject to effective independent oversight mechanisms […]

Concluding Observations on the Seventh Periodic Report of Germany, Human Rights Committee, UN Doc CCPR/C/DEU/CO/7 (11 November 2021)

42. The Committee is concerned about the wide reaching powers of surveillance, including online surveillance and the hacking of encrypted communications data during criminal investigations. […]

43. The State party should also ensure that surveillance is subject to effective independent oversight mechanisms, namely judicial, […]

Concluding Observations on the Fourth Periodic Report of Bulgaria, Human Rights Committee, UN Doc CCPR/C/BGR/CO/4 (15 November 2018)

34. The State party should review its legislation in order to bring it into line with its obligations under the Covenant. It should, in particular: […] (c) Ensure that surveillance activities conform with its obligations under article 17 of the Covenant, including […] that they are subject to periodic judicial review […]

Concluding Observations on the Seventh Periodic Report of Norway, Human Rights Committee, UN Doc CCPR/C/NOR/CO/7 (25 April 2018)

21. […] [The State party] should also ensure the effectiveness and independence of a monitoring system for surveillance activities.

Concluding Observations on the Initial Report of Pakistan, Human Rights Committee, UN Doc CCPR/C/PAK/CO/1 (27 July 2017)

35. While noting the State party's view that the Prevention of Electronic Crimes Act 2016 complies with the Convention on Cybercrime, the Committee is concerned that the Act provides for (a) overbroad powers to the Pakistan Telecommunication Authority and the authorized officers without sufficient independent judicial oversight mechanisms. [...]

36. The State party should review its legislation on data collection and surveillance, in particular, the Prevention of Electronic Crimes Act 2016, to bring it in line with its obligations under the Covenant. It should also establish independent oversight mechanisms on the implementation of the Act, including judicial review of surveillance activity. […]

Concluding Observations on the Sixth Periodic Report of Morocco, Human Rights Committee, UN Doc CCPR/C/MAR/CO/6 (4 November 2016)

38. […] The State party should also establish independent oversight mechanisms in order to prevent abuses.

Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee, UN Doc CCPR/C/POL/CO/7 (4 November 2016)

39. […] The Committee is particularly concerned about: d) the lack of adequate judicial oversight;

Concluding Observations on the Seventh Periodic Report of the Russian Federation, Human Rights Committee, UN Doc CCPR/C/RUS/CO/7 (28 April 2015)

13. The Committee regrets the lack of clarity as to whether the 2006 Federal Counter-Terrorism Act: […] (c) provides for independent review of counter-terrorism activities undertaken by the executive, including with regard to monitoring telephone, electronic and postal communications. [...] The State party should also ensure that its counter-terrorism legislation provides for an independent mechanism to review counter-terrorism activities undertaken by the executive.

Committee on the Elimination of Racial Discrimination, General Recommendation No 36 (2020) on Preventing and Combating Racial Profiling by Law Enforcement Officials, UN Doc CERD/C/GC/36 (17 December 2020)

62. States should adopt measures to ensure that independent oversight bodies have a mandate to monitor the use of artificial intelligence tools by the public sector, and to assess them against criteria developed in conformity with the Convention to ensure they are not entrenching inequalities or producing discriminatory results. States should also ensure that the functioning of such systems is regularly monitored and evaluated in order to assess deficiencies and to take the necessary corrective measures. When the results of an assessment of a technology indicate a high risk of discrimination or other human rights violations, States should take measures to avoid the use of such a technology.

Commissioner for Human Rights, Council of Europe, Positions on Counter-Terrorism and Human Rights Protection, CommDH/PositionPaper(2015)1 (5 June 2015)

States should establish or designate one or more bodies that are fully independent from the executive and the security services to oversee all aspects of security service regulations, policies, operations, data collection and administration, and ensure that their systems for the oversight of security services comply with human rights requirements. […]

States should consider the introduction of security-cleared public interest advocates into surveillance authorisation processes, create or designate an independent, external oversight body to receive and investigate complaints relating to all aspects of security service activity, and give an external oversight body the power to quash surveillance measures when such activities are deemed to have been unlawful. Independent, external bodies responsible for scrutinising security services should publish public versions of their periodic and investigation reports...

Commissioner for Human Rights, Council of Europe, Issue Paper on Democratic and Effective Oversight of National and Security Services, Commissioner's Recommendations (May 2015)

1. Establish or designate one or more bodies that are fully independent from the executive and the security services to oversee all aspects of security service regulations, policies, operations and administration. […]

4. Ensure that the oversight of security services focuses not only on the lawfulness of security service activities that restrict the right to privacy and family life but also the rights to freedom of expression, assembly, association and religion, thought and conscience.

5. Mandate oversight bodies to scrutinise the human rights compliance of security service co-operation with foreign bodies, including co-operation through the exchange of information, joint operations and the provision of equipment and training. External oversight of security service co-operation with foreign bodies should include but not be limited to examining: (a) ministerial directives and internal regulations relating to international intelligence cooperation; (b) human rights risk assessment and risk-management processes relating to relationships with specific foreign security services and to specific instances of operational co-operation; (c) outgoing personal data and any caveats (conditions) attached thereto; (d) security service requests made to foreign partners: (i) for information on specific persons; and (ii) to place specific persons under surveillance; (e) intelligence co-operation agreements; (f) joint surveillance operations and programmes undertaken with foreign partners.

7. Require that security services obtain authorisation from a body that is independent from the security services and the executive, both in law and in practice, before engaging in any of the following activities either directly or through/in collaboration with private sector entities: (a) conducting untargeted bulk surveillance measures regardless of the methods or technology used or the type of communications targeted; (b) using selectors or key words to extract data from information collected through bulk surveillance, particularly when these selectors relate to identifiable

persons; (c) collecting communications/metadata directly or accessing it through requests made to third parties, including private companies; (d) accessing personal data held by other state bodies; (e) undertaking computer network exploitation.

8. Ensure that, where security services engage in computer network exploitation, these activities are subject to the same level of external oversight as is required for surveillance measures that have equivalent human rights implications.

9. Consider the introduction of security-cleared public interest advocates into surveillance authorisation processes, including both targeted and untargeted surveillance measures, to represent the interests of would-be targets of surveillance.

10. Consider how surveillance authorisation processes can be kept under ex post facto review by an independent body that is empowered to examine decisions taken by the authorising body.

11. Create or designate an external oversight body to receive and investigate complaints relating to all aspects of security service activity. Where such bodies are only empowered to issue non-binding recommendations, member states must ensure that complainants also have recourse to another institution that can provide remedies that are effective both in law and in practice.

12. Give an external oversight body the power to quash surveillance warrants and discontinue surveillance measures undertaken without the need for a warrant when such activities are deemed to have been unlawful, as well as the power to require the deletion of any information obtained from the use of such measures.

13. Ensure that the procedures of any institution tasked with adjudicating on complaints relating to matters that have been revealed to a complainant or otherwise made public comply with due process standards under European human rights law."

***Ekimdzhiev and Ors v Bulgaria*, App No 70078/12, Judgment, European Court of Human Rights (11 January 2022)**

334. The relevant factors for deciding whether the oversight arrangements are adequate are (a) the independence of the supervisory authorities, their competences, and their powers (both to access materials and to redress breaches, in particular order the destruction of surveillance materials), and (b) the possibility of effective public scrutiny of those authorities' work.

335. In Bulgaria, three authorities can supervise the use of special means of surveillance: (a) the judge who has issued the respective surveillance warrant; (b) the National Bureau; and (c) a special parliamentary committee (see paragraphs 106 to 135 above).

336. […] It nevertheless falls short of the requisite standard of effectiveness in several aspects.

337. […] in all instances of surveillance outside already pending criminal proceedings that judge has no power to order remedial measures, such as the destruction of surveillance materials. More importantly, he or she is not empowered or expected to carry out on-site inspections, and performs his or her supervisory duties solely on the basis of the report submitted by the authorities. […]

338. For its part, the main supervisory body, the National Bureau, suffers from several shortcomings undermining its effectiveness in practice.

339. First, there is no guarantee that all of its members are sufficiently independent *vis-à-vis* the authorities which they must oversee. […] By law, individuals with professional experience in the law-enforcement or the security services may become members of the National Bureau (see paragraph 109 above). After serving their five-year term (which, granted, can be renewed), they are entitled to

regain their previous posts (see paragraph 111 above). This potential "revolving door" mechanism can raise misgivings about the practical independence of such members of the Bureau and about possible conflicts of interests on their part (see, *mutatis mutandis*, *Centrum för rättvisa*, cited above, § 359).

340. […] Before being appointed to their posts, its members must undergo security vetting by one of the very authorities whose work the Bureau is overseeing – the State Agency for National Security (see paragraphs 109 and 110 above). This creates an obvious conflict of interests for that Agency. […]

342. Secondly, misgivings arise about the qualifications of some of the members of the National Bureau. Only one of its current five members has legal training and experience […]

343. Thirdly, it does not appear that when carrying out on-site inspections members of the National Bureau and its employees are able to have unfettered access to all relevant materials held by the prosecuting authorities and the State Agency for National Security, especially materials enabling them to check the well-foundedness of surveillance applications (reasonable suspicion and proportionality in each case) […]

344. Lastly, the National Bureau has no power to order remedial measures, such as the destruction of surveillance materials. […]

345. The special parliamentary committee is not empowered to order remedial measures either (see paragraph 127 above). Moreover, unlike the National Bureau, it does not appear to conduct regular inspections […]

347. In view of the defects outlined above, the system of overseeing secret surveillance in Bulgaria as it is currently organised does not appear capable of providing effective guarantees against abusive surveillance.

410. In Bulgaria, three authorities can oversee the retention of communications data and its subsequent accessing by the authorities: (a) the Commission for Protection of Personal Data; (b) the judge who has issued the access warrant; and (c) the same parliamentary committee which oversees secret surveillance (see paragraphs 197 to 210 above).

411. […] mandate [of the Commission for Protection of Personal Data] under the 2007 Act appears to be limited to overseeing communications service providers (see paragraph 198 above); it has no express powers under that Act with respect to the authorities which can access retained communications data.

412. It is true that under the provisions of the 2002 Act, as amended in 2019 to transpose Directive (EU) 2016/680, the same Commission – as well as the Inspectorate attached to the Supreme Judicial Council – are tasked with supervising the way in which the authorities process any personal data for law-enforcement purposes (see paragraph 225 above). But nothing suggests that either of those two authorities has so far availed itself of those powers in relation to communications data.

413. […] that judge has no power to order remedial measures. He or she is, moreover, not empowered or expected to carry out on-site inspections, and performs his or her supervisory duties solely on the basis of the report submitted by the authorities. […]

414. […] First, […] members [of the special parliamentary committee] need not be persons with legal qualifications or experience (see paragraph 206 above). Secondly, it has no power to order remedial measures in concrete cases, such as the destruction of retained or accessed communications data; it can only give instructions designed to improve the relevant procedures (see paragraph 211 above). If it detects irregularities, it can only bring the matter to the attention of the prosecuting authorities,

or inform the heads of the relevant access-requesting authorities and communications service providers (see paragraph 212 above).

415. In view of the shortcomings outlined above, the system of overseeing the retention of communications data and its subsequent accessing by the authorities in Bulgaria, as currently organised, does not appear capable of providing effective guarantees against abusive practices in this respect.

***Big Brother Watch and Others v The United Kingdom*, Apps Nos 58170/13, 62322/14 and 24960/15, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

349. […] In the context of bulk interception the importance of supervision and review will be amplified, because of the inherent risk of abuse and because the legitimate need for secrecy will inevitably mean that, for reasons of national security, States will often not be at liberty to disclose information concerning the operation of the impugned regime.

356. Each stage of the bulk interception process – including the initial authorisation and any subsequent renewals, the selection of bearers, the choice and application of selectors and query terms, and the use, storage, onward transmission and deletion of the intercept material – should also be subject to supervision by an independent authority and that supervision should be sufficiently robust to keep the "interference" to what is "necessary in a democratic society" (see *Roman Zakharov*, cited above, § 232; see also *Klass and Other*, cited above, §§ 49, 50 and 59; *Weber and Saravia*, cited above, § 106 and *Kennedy*, cited above, §§ 153 and 154). In particular, the supervising body should be in a position to assess the necessity and proportionality of the action being taken, having due regard to the corresponding level of intrusion into the Convention rights of the persons likely to be affected. In order to facilitate this supervision, detailed records should be kept by the intelligence services at each stage of the process.

362. […] Finally, the Court considers that the transfer of material to foreign intelligence partners should also be subject to independent control.

***Centrum för Rättvisa v Sweden*, App No 35252/08, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

250. […] Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In a field where abuse in individual cases is potentially so easy and could have such harmful consequences for democratic society as a whole, the Court has held that it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure […].

270. Each stage of the bulk interception process – including the initial authorisation and any subsequent renewals, the selection of bearers, the choice and application of selectors and query terms, and the use, storage, onward transmission and deletion of the intercept material – should also be subject to supervision by an independent authority and that supervision should be sufficiently robust to keep the "interference" to what is "necessary in a democratic society" (see *Roman Zakharov*, cited above, § 232; see also *Klass and Others*, cited above, §§ 49, 50 and 59; *Weber and Saravia*, cited above, § 106; and *Kennedy*, cited above, §§ 153 and 154). In particular, the supervising body should be in a position to assess the necessity and proportionality of the action being taken, having due regard to the corresponding level of intrusion into the Convention rights of the persons likely to be affected. In order to facilitate this supervision, detailed records should be kept by the intelligence services at each stage of the process.

***Ivashchenko v Russia*, App No 61064/10, Judgment, European Court of Human Rights (13**

February 2018)

74. […], the existence of sufficient procedural safeguards may be particularly pertinent, having regard to, to some extent at least and among other factors, the nature and extent of the interference in question. In various contexts of Article 8 of the Convention, the Court has emphasised that measures affecting human rights must be subject to some form of adversarial proceedings before an independent body competent to review in a timely fashion the reasons for the decision and the relevant evidence.

***Szabó and Vissy v Hungary*, App No 37138/14, Judgment, European Court of Human Rights (12 January 2016)**

79. It is in this context that the external, preferably judicial, a posteriori control of secret surveillance activities, both in individual cases and as general supervision, gains its true importance, by reinforcing citizens' trust that guarantees of the rule of law are at work even in this sensitive field and by providing redress for any abuse sustained. The significance of this control cannot be overestimated in view of the magnitude of the pool of information retrievable by the authorities applying highly efficient methods and processing masses of data, potentially about each person, should he be, one way or another, connected to suspected subjects or objects of planned terrorist attacks. The Court notes the lack of such a control mechanism in Hungary.

85. In any event, the Court recalls that in *Klass and Others* a combination of oversight mechanisms, short of formal judicial control, was found acceptable in particular because of "an initial control effected by an official qualified for judicial office". However, the Hungarian scheme of authorisation does not involve any such official. The Hungarian Commissioner for Fundamental Rights has not been demonstrated to be a person who necessarily holds or has held a judicial office.

88. Lastly, the Court notes that is for the Government to illustrate the practical effectiveness of the supervision arrangements with appropriate examples. However, the Government were not able to do so in the instant case.

***Roman Zakharov v Russia*, App No 47143/06, Judgment, European Court of Human Rights (4 December 2015)**

273. As regards supervision of interceptions carried out on the basis of proper judicial authorisations, the Court will examine whether the supervision arrangements existing in Russia are capable of ensuring that the statutory requirements relating to the implementation of the surveillance measures, the storage, access to, use, processing, communication and destruction of intercept material are routinely respected.

274. A court which has granted authorisation for interception has no competence to supervise its implementation. It is not informed of the results of the interceptions and has no power to review whether the requirements of the decision granting authorisation were complied with. Nor do Russian courts in general have competence to carry out the overall supervision of interceptions. Judicial supervision is limited to the initial authorisation stage. Subsequent supervision is entrusted to the President, Parliament, the Government, the Prosecutor General and competent lower-level prosecutors.

275. The Court has earlier found that, although it is in principle desirable to entrust supervisory control to a judge, supervision by non-judicial bodies may be considered compatible with the Convention, provided that the supervisory body is independent of the authorities carrying out the surveillance, and is vested with sufficient powers and competence to exercise an effective and continuous control.

276. As far as the President, Parliament and the Government are concerned, Russian law does not set out the manner in which they may supervise interceptions. There are no publicly available

regulations or instructions describing the scope of their review, the conditions under which it may be carried out, the procedures for reviewing the surveillance measures or for remedying the breaches detected.

277. As regards supervision of interceptions by prosecutors, the Court observes that the national law sets out the scope of, and the procedures for, prosecutors' supervision of operational-search activities. It stipulates that prosecutors may carry out routine and ad hoc inspections of agencies performing operational-search activities and are entitled to study the relevant documents, including confidential ones. They may take measures to stop or remedy the detected breaches of law and to bring those responsible to liability. They must submit semi-annual reports detailing the results of the inspections to the Prosecutor General's Office. The Court accepts that a legal framework exists which provides, at least in theory, for some supervision by prosecutors of secret surveillance measures. It must be next examined whether the prosecutors are independent of the authorities carrying out the surveillance, and are vested with sufficient powers and competence to exercise effective and continuous control.

278. As to the independence requirement, in previous cases the Court has taken into account the manner of appointment and the legal status of the members of the supervisory body. In particular, it found sufficiently independent the bodies composed of members of parliament of both the majority and the opposition, or of persons qualified to hold judicial office, appointed either by parliament or by the Prime Minister. In contrast, a Minister of Internal Affairs – who not only was a political appointee and a member of the executive, but was directly involved in the commissioning of special means of surveillance – was found to be insufficiently independent. Similarly, a Prosecutor General and competent lower-level prosecutors were also found to be insufficiently independent.

279. In contrast to the supervisory bodies cited above, in Russia prosecutors are appointed and dismissed by the Prosecutor General after consultation with the regional executive authorities. This fact may raise doubts as to their independence from the executive.

280. Furthermore, it is essential that any role prosecutors have in the general protection of human rights does not give rise to any conflict of interest. The Court observes that prosecutor's offices do not specialise in supervision of interceptions. Such supervision is only one part of their broad and diversified functions, which include prosecution and supervision of criminal investigations. In the framework of their prosecuting functions, prosecutors give their approval to all interception requests lodged by investigators in the framework of criminal proceedings. This blending of functions within one prosecutor's office, with the same office giving approval to requests for interceptions and then supervising their implementation, may also raise doubts as to the prosecutors' independence.

281. Turning now to the prosecutors' powers and competences, the Court notes that it is essential that the supervisory body has access to all relevant documents, including closed materials and that all those involved in interception activities have a duty to disclose to it any material it required. Russian law stipulates that prosecutors are entitled to study relevant documents, including confidential ones. It is however important to note that information about the security services' undercover agents, and about the tactics, methods and means used by them, is outside the scope of prosecutors' supervision.

282. The supervisory body's powers with respect to any breaches detected are also an important element for the assessment of the effectiveness of its supervision. The Court is satisfied that prosecutors have certain powers with respect to the breaches detected by them. Thus, they may take measures to stop or remedy the detected breaches of law and to bring those responsible to liability. However, there is no specific provision requiring destruction of the unlawfully obtained intercept material.

283. The Court must also examine whether the supervisory body's activities are open to public scrutiny. In Russia, prosecutors must submit semi-annual reports detailing the results of the

inspections to the Prosecutor General's Office. However, these reports concern all types of operational-search measures, amalgamated together, without interceptions being treated separately from other measures. Moreover, the reports contain only statistical information about the number of inspections of operational-search measures carried out and the number of breaches detected, without specifying the nature of the breaches or the measures taken to remedy them. It is also significant that the reports are confidential documents. They are not published or otherwise accessible to the public. It follows that in Russia supervision by prosecutors is conducted in a manner which is not open to public scrutiny and knowledge.

284. Lastly, the Court notes that it is for the Government to illustrate the practical effectiveness of the supervision arrangements with appropriate examples. However, the Russian Government did not submit any inspection reports or decisions by prosecutors ordering the taking of measures to stop or remedy a detected breach of law. It follows that the Government did not demonstrate that prosecutors' supervision of secret surveillance measures is effective in practice. The Court also takes note in this connection of the documents submitted by the applicant illustrating prosecutors' inability to obtain access to classified materials relating to interceptions. That example also raises doubts as to the effectiveness of supervision by prosecutors in practice.

285. In view of the defects identified above, and taking into account the particular importance of supervision in a system where law-enforcement authorities have direct access to all communications, the Court considers that the prosecutors' supervision of interceptions as it is currently organised is not capable of providing adequate and effective guarantees against abuse.

***Kennedy v The United Kingdom*, App No 26839/05, Judgment, European Court of Human Rights (18 May 2010)**

166. As regards supervision of the RIPA regime, the Court observes that apart from the periodic review of interception warrants and materials by intercepting agencies and, where appropriate, the Secretary of State, the Interception of Communications Commissioner established under RIPA is tasked with overseeing the general functioning of the surveillance regime and the authorisation of interception warrants in specific cases. He has described his role as one of protecting members of the public from unlawful intrusion into their private lives, of assisting the intercepting agencies in their work, of ensuring that proper safeguards are in place to protect the public and of advising the Government and approving the safeguard documents. The Court notes that the Commissioner is independent of the executive and the legislature and is a person who holds or has held high judicial office. He reports annually to the Prime Minister and his report is a public document (subject to the non-disclosure of confidential annexes) which is laid before Parliament. In undertaking his review of surveillance practices, he has access to all relevant documents, including closed materials and all those involved in interception activities have a duty to disclose to him any material he requires. The obligation on intercepting agencies to keep records ensures that the Commissioner has effective access to details of surveillance activities undertaken. The Court further notes that, in practice, the Commissioner reviews, provides advice on and approves the section 15 arrangements. The Court considers that the Commissioner's role in ensuring that the provisions of RIPA and the Code are observed and applied correctly is of particular value and his biannual review of a random selection of specific cases in which interception has been authorised provides an important control of the activities of the intercepting agencies and of the Secretary of State himself.

167. The Court recalls that it has previously indicated that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge. In the present case, the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems, any person who suspects that his communications have been or are being intercepted may apply to the IPT. The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications. The Court emphasises that the IPT is an independent and

impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high judicial office or be experienced lawyers. In undertaking its examination of complaints by individuals, the IPT has access to closed material and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the authorisation and execution of a warrant of all documents it considers relevant. In the event that the IPT finds in the applicant's favour, it can, inter alia, quash any interception order, require destruction ofintercept material and order compensation to be paid. The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom

168. Finally, the Court observes that the reports of the Commissioner scrutinise any errors which have occurred in the operation of the legislation. In his 2007 report, the Commissioner commented that none of the breaches or errors identified were deliberate and that, where interception had, as a consequence of human or technical error, unlawfully taken place, any intercept material was destroyed as soon as the error was discovered. There is therefore no evidence that any deliberate abuse of interception powers is taking place.

169. In the circumstances, the Court considers that the domestic law on interception of internal communications together with the clarifications brought by the publication of the Code indicate with sufficient clarity the procedures for the authorisation and processing of interception warrants as well as the processing, communicating and destruction of intercept material collected. The Court further observes that there is no evidence of any significant shortcomings in the application and operation of the surveillance regime. On the contrary, the various reports of the Commissioner have highlighted the diligence with which the authorities implement RIPA and correct any technical or human errors which accidentally occur. Having regard to the safeguards against abuse in the procedures as well as the more general safeguards offered by the supervision of the Commissioner and the review of the IPT, the impugned surveillance measures, insofar as they may have been applied to the applicant in the circumstances outlined in the present case, are justified under Article 8 § 2."

***Rotaru v Romania*, App No 28341/95, Judgment, European Court of Human Rights (4 May 2000)**

59. The Court must also be satisfied that there exist adequate and effective safeguards against abuse, since a system of secret surveillance designed to protect national security entails the risk of undermining or even destroying democracy on the ground of defending it. In order for systems of secret surveillance to be compatible with Article 8 of the Convention, they must contain safeguards established by law which apply to the supervision of the relevant services' activities. Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure.

***Klass and Others v Germany*, App No 5029/71, Judgment, European Court of Human Rights (6 September 1978)**

54. The Government maintains that Article 8 para. 2 (art. 8-2) does not require judicial control of secret surveillance and that the system of review established under the G 10 does effectively protect the rights of the individual. The applicants, on the other hand, qualify this system as a "form of political control", inadequate in comparison with the principle of judicial control which ought to prevail. It therefore has to be determined whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" resulting from the contested legislation to what is "necessary in a democratic society"

55. Review of surveillance may intervene at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual's rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 para. 2 (art. 8-2), are not to be exceeded. One of the fundamental principles of a democratic society is the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure.

56. Within the system of surveillance established by the G 10, judicial control was excluded, being replaced by an initial control effected by an official qualified for judicial office and by the control provided by the Parliamentary Board and the G 10 Commission. The Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge. Nevertheless, having regard to the nature of the supervisory and other safeguards provided for by the G 10, the Court concludes that the exclusion of judicial control does not exceed the limits of what may be deemed necessary in a democratic society. The Parliamentary Board and the G 10 Commission are independent of the authorities carrying out the surveillance, and are vested with sufficient powers and competence to exercise an effective and continuous control. Furthermore, the democratic character is reflected in the balanced membership of the Parliamentary Board. The opposition is represented on this body and is therefore able to participate in the control of the measures ordered by the competent Minister who is responsible to the Bundestag. The two supervisory bodies may, in the circumstances of the case, be regarded as enjoying sufficient independence to give an objective ruling."

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet OEA/Ser.L/V/II. CIDH/RELE/INF.11/13 (31 December 2013)

150. […]. Moreover, the people most affected are those who take unpopular positions, or the members of political, racial, or religious minorities who are often unjustifiably classified as "terrorists," which makes them the object of surveillance and monitoring without proper oversight. [...]

***Ligue des droits humains v Conseil des ministres* (C-817/19), Judgment, Grand Chamber, Court of Justice of the European Union (21 June 2022)**

172. The decision providing for that application must be open to effective review, either by a court or by an independent administrative body whose decision is binding, in order to verify that that situation exists and that the conditions and safeguards which must be laid down are observed. The period of application must also be limited in time to what is strictly necessary but may be extended if that threat persists (see, by analogy, judgments of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168, and of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 58).

***La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées; Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministers (C-511/18, C-512/18 and C-520/18)*, Judgment,**

Grand Chamber, Court of Justice of the European Union (6 October 2020)

192. […] Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as not precluding national rules which requires providers of electronic communications services to have recourse, first, to the automated analysis and real-time collection, inter alia, of traffic and location data and, second, to the real-time collection of technical data concerning the location of the terminal equipment used, where: […] recourse to automated analysis is limited to situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and where recourse to such analysis may be the subject of an effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that a situation justifying that measure exists and that the conditions and safeguards that must be laid down are observed; […]

***Draft Agreement between Canada and the European Union on the Transfer of Passenger Name Record data (1/15)*, Court of Justice of the European Union, Grand Chamber, Opinion pursuant to Article 218(11) TFEU (26 July 2017)**

229. In accordance with the settled case-law of the Court, the guarantee of the independence of [a] supervisory authority [...] is intended to ensure the effectiveness and reliability of the monitoring of compliance with the rules concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. The establishment of an independent supervisory authority is therefore an essential component of the protection of individuals with regard to the processing of personal data.

***Tele2 Sverige AB v Post- Och telestyrelsen* (C-203/15); *Secretary of State for the Home Department v Tom Watson et al.* (C-698/16), Joined Cases, Judgment, Grand Chamber, Court of Justice of the European Union (21 December 2016)**

120. In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime. [...]

123. In any event, the Member States must ensure review, by an independent authority, of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly required by Article 8(3) of the Charter and constituting, in accordance with the Court's settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data.

***Maximillian Schrems v Data Protection Commissioner* (C-362/14), Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2015)**

39. It is apparent from Article 1 of Directive 95/46 and recitals 2 and 10 in its preamble that that directive seeks to ensure not only effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the fundamental right to respect for private life with regard to the processing of personal data, but also a high level of protection of those fundamental rights and freedoms [...]

40. As regards the powers available to the national supervisory authorities in respect of transfers of personal data to third countries, it should be noted that Article 28(1) of Directive 95/46 requires

Member States to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of such data. In addition, that requirement derives from the primary law of the European Union, in particular Article 8(3) of the Charter and Article 16(2) TFEU.

41. The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities. The establishment in Member States of independent supervisory authorities is therefore, as stated in recital 62 in the preamble to Directive 95/46, an essential component of the protection of individuals with regard to the processing of personal data.

42. In order to guarantee that protection, the national supervisory authorities must, in particular, ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other hand, the interests requiring free movement of personal data.

43. The national supervisory authorities have a wide range of powers for that purpose. Those powers, listed on a non-exhaustive basis in Article 28(3) of Directive 95/46, constitute necessary means to perform their duties, as stated in recital 63 in the preamble to the directive. Thus, those authorities possess, in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings.

IV. DATA PROTECTION IN SURVEILLANCE

The following sub-section contains references to statements by human rights mechanisms which depict primarily how general principles of data protection are relevant to safeguards pertaining surveillance. The sub-section is interlinked to the section of the Guide on mass surveillance, where references to statements and jurisprudence relating to bulk data retention may be found, as well as the one on biometric data processing.

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

Expressing concern that individuals, particularly children, often do not and/or cannot provide their free, explicit and informed consent to the collection, processing and storage of their data or to the reuse, sale or multiple resale of their personal data, as the collection, processing, use, storage and sharing of personal data, including sensitive data, have increased significantly in the digital age,

7. *Calls upon* all States: (o) To protect individuals from violations or abuses of the right to privacy, including those which are caused by arbitrary or unlawful data collection, processing, storage and sharing, profiling and the use of automated processes and machine learning;

** See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166*

(18 December 2014)

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)

Expressing concern that individuals, in particular children, often do not and/or cannot provide their free, explicit and informed consent to the collection, processing and storage of their data or to the reuse, sale or multiple resale of their personal data, as the collecting, processing, use, storage and sharing of personal data, including sensitive data, have increased significantly in the digital age, and that if personal and sensitive data are disclosed, exceptional damage, injury or hardship may be caused to individuals,

3. *Also affirms* that, in order to protect, respect and promote the right to privacy, personal data should only be collected for specified, explicit and legitimate purposes and must be processed lawfully, fairly and in a transparent manner;

4. *Highlights* that every person should be able to ascertain which public authorities or private individuals or bodies control or may control their personal data, and that any interference with data protection must be lawful, in accordance with international human rights law, including the principles of legality, proportionality, necessity and non-discrimination;

8. *Calls upon* States:

(h) To develop or maintain and implement adequate legislation, with effective sanctions and remedies, that protects individuals against violations and abuses of the right to privacy, namely through the collection, processing, retention or use of personal data by individuals, Governments, business enterprises or private organizations without the individual's free, explicit and informed consent or unless otherwise lawful, in accordance with international human rights law;

(i) To consider adopting or maintaining data protection legislation, regulations and policies, including on digital communication data, that comply with their international human rights obligations and that could include provisions on sensitive personal data protection and the establishment of national independent authorities with the powers and resources to monitor data privacy practices, investigate violations and abuses and receive communications from individuals and organizations, and to provide appropriate effective remedies;

Report of the United Nations High Commissioner for Human Rights, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests, UN Doc A/HRC/44/24 (24 June 2020)

53. In this context, the High Commissioner recommends that States:

(j) Establish a moratorium on the use of facial recognition technology in the context of peaceful assemblies, at least until the authorities responsible can demonstrate compliance with privacy and data protection standards as well as the absence of significant accuracy issues and discriminatory impacts, and until the following recommendations are implemented:

(iii) Put in place strict privacy and data protection laws that regulate the collection, retention, analysis and otherwise processing of personal data, including facial templates;

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/29/32 (22 May 2015)

55. Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint. A State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information.

***Weber and Saravia v Germany*, App No 54934/00, Decision, European Court of Human Rights (29 June 2006)**

132. The Court notes in the first place that the impugned provisions, in providing for the destruction of personal data as soon as they were no longer needed to achieve their statutory purpose, and for the verification at regular, fairly short intervals of whether the conditions for such destruction were met, constituted an important element in reducing the effects of the interference with the secrecy of telecommunications to an unavoidable minimum.

UN General Assembly Resolution on the Rights of the Children, UN Doc A/RES/78/187 (19 December 2023)

Expressing concern that children often do not and/or cannot provide their free, explicit and informed consent to the collection, processing and storage of their data or to the reuse, sale or multiple resale of their personal information, as the collection, processing, use, storage and sharing of personal information, including sensitive data, have increased significantly in the digital age,

43. *Urges* States to prohibit the unlawful digital surveillance of children, with due regard to commercial settings and educational and care settings, to work towards enabling secure communications and the protection of individual users against arbitrary or unlawful interference with their privacy, including by developing technical solutions with any restrictions thereon complying with the obligations of States under relevant international human rights instruments;

UN General Assembly Resolution on the Promotion and Protection of Human Right in the Context of Digital Technologies, UN Doc A/RES/78/213 (19 December 2023)

Noting also that the use of data collection, data extraction and algorithms to target content towards online users may undermine user agency and access to information online, and noting further that the collection, processing, use, storage and sharing of personal data, including for reuse, sale or multiple resale, risks infringing on the user's human rights,

UN General Assembly Resolution on the United Nations Global Counter-Terrorism Strategy: eighth review, UN Doc A/RES/77/298 (22 June 2023)

111. *Calls upon* States, while countering terrorism and preventing violent extremism conducive to terrorism, to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, by ensuring the full and effective implementation of all their obligations under international human rights law;

UN Human Rights Council Resolution on Freedom of Opinion and Expression, UN Doc A/HRC/RES/50/15 (8 July 2022)

8. *Calls upon* all States: (p) To adopt, implement and, where necessary, reform laws, regulations,

policies and other measures concerning personal data and privacy protection online in order to prevent, mitigate and remedy the arbitrary or unlawful collection, retention, processing, use or disclosure of personal data on the Internet that could violate human rights and deter individuals from the full exercise of their rights to freedom of opinion and expression;

Report of the Working Group on Enforced and Involuntary Disappearances, 'New technologies and enforced disappearances', UN Doc A/HRC/54/22/Add.5 (11 September 2023)

49. Finding and piercing together corroborating information through technologies – and especially ICT – requires formidable efforts in terms of targeted investigation, verification and preservation, which should always be done in a systematic and professional manner, especially to ensure the chain of custody and, where necessary, admissibility in court at a later stage. Throughout the process, from the collection of evidence through technologies until its appearance in court, ethical and security implications must be adequately taken into account. In particular, risk-assessment should include consideration of privacy and data protection aspects, the obtaining – where feasible – of informed consent from relevant individuals and communities and Demographically Identifiable Data-based risks.

Report of the Special Rapporteur on contemporary forms of slavery, including its causes and consequences, UN Doc A/78/161 (12 July 2023)

41. […] Many of the technology tools developed to counter and prevent contemporary forms of slavery collect, store and analyse a large volume of sensitive data, including personal information of victims and exploiters, such as their real facial images, names, addresses, telephone numbers and credit card or bank account information. Such data can be obtained illegally through cyberattacks or fraud and misused by traffickers and exploiters to their advantage. This underscores the need to tighten cybersecurity by establishing sufficient safeguards against the mishandling of such information. […]

Report of the Working Group on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination, Impact of the Use of Private Military and Security Services in Immigration and Border Management on the Protection of the Rights of All Migrants, UN Doc A/HRC/45/9 (9 July 2020)

41. In the absence of adequate privacy safeguards in many countries, there are risks that data is gathered in a non-transparent manner and without informed consent, stored for long periods, and becomes outdated even while the database is still in use. Decisions taken during screening processes for migrants, including refugees and asylum seekers, that rely heavily on such technology with its presumed rationality and superiority, lack nuanced human judgment and risk potentially serious errors. Given the high-tech nature of such systems, States may lack adequate legislation, knowledge and expertise to provide effective oversight of these operations. Moreover, abuses of the right to privacy generated by these systems are likely to go underreported as migrants may be unaware of their rights or unable to exercise them due to the vulnerable situations in which they find themselves.

Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, Racial Discrimination and Emerging Digital Technologies: a Human Rights Analysis, UN Doc A/HRC/44/57 (18 June 2020)

49. […] The Special Rapporteur urges States to adopt an approach to data grounded in human rights, by ensuring disaggregation, self-identification, transparency, privacy, participation and accountability in the collection and storage of data. […]

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/43/52 (24 March 2020)

42. States and non-State actors should ensure the highest attainable standard of data protection for all individuals, regardless of their gender, by:

(a) Adopting best practice data protection laws and regulation, including the establishment of a well-resourced, independent privacy or data regulator with appropriate powers and public reporting mechanisms;

(b) Developing systems for the effective protection and use of data in ways that benefit society and all individuals, regardless of their gender;

(g) Employing the principles of data minimization, necessity and proportionality when aggregating gender data so that only the minimum necessary level of detail is included in a data set to achieve the intended positive outcome of the use of the data;

(h) Taking appropriate and necessary measures to guarantee the confidentiality and security of the personal data of individuals vulnerable on account of their gender, such as same-sex couples;

(i) Prohibiting the release of unit record data on sex or gender as open data;

(j) Protecting personal information relating to sex and gender through regular vulnerability assessments of information management systems and regular training for staff on data privacy and data security;

(k) Using privacy impact assessments and other mechanisms to ensure that data analytics do not result in inferences being drawn about individuals or groups according to their gender, which could lead to discrimination.

Report of the Working Group of Experts on People of African Descent on its Twenty-Third and Twenty-Fourth Sessions, UN Doc A/HRC/42/59 (15 August 2019)

83. The Working Group urges Member States to adopt a human rights-based approach to data, by providing for disaggregation, self-identification, transparency, privacy, participation and accountability in collecting and storing data."

Report of the Independent Expert on the Protection Against Violence and Discrimination Based on Sexual Orientation and Gender Identity, Data Collection and Management as a Means to Create Heightened Awareness of Violence and Discrimination Based on Sexual Orientation and Gender Identity, UN Doc A/HRC/41/45 (14 May 2019)

55. The principle of lawful use limits the use of data to those purposes provided for by law, including international human rights law, and limits access to data to those individuals whose involvement is necessary to accomplish those purposes. This is particularly important when data is collected for the purposes of administering programmes, delivering services, enforcing law and evaluating programmes. In such cases, individuals may not be directly informed about how their data will be used and maintained, and may not be provided with an opportunity to consent to such use.

56. Conversely, the collection and management of data to enable criminal prosecution of same-sex relations or on the basis of sexual orientation and gender identity is, by definition, a violation of the principle of lawful use. The mandate holder has already concluded that legislation, public policy and jurisprudence that criminalize same-sex relationships and particular gender identities are per se contrary to international human rights law, and therefore any measures, including data collection and management, conducive to their implementation are equally contrary to international human rights law.

Concluding Observations on the Fifth Periodic Report of the United States of America, Human Rights Committee, UN Doc CCPR/C/USA/CO/5 (30 October 2023)

56. […] The Committee is also concerned at reports that government agencies, such as Immigration and Customs Enforcement, have used databases of personal information systematically collected by private entities without the consent of the individuals concerned, in particular for surveillance purposes, without proper mechanisms for protecting the right to privacy (art. 2, 17 and 26).

Concluding Observations on the Initial Report of the State of Palestine, Human Rights Committee, UN Doc CCPR/C/PSE/CO/1 (21 July 2023)

38. In the light of the Committee's general comment No. 16 (1988) on right to privacy, the State party should: (b) Bring regulations governing data retention and access, surveillance and interception activities into conformity with the Covenant, and ensure strict adherence to the principles of legality, proportionality and necessity; (c) Ensure that no personal data is shared arbitrarily;

Concluding Observations on the Fourth Periodic Report of Hong Kong, China, Human Rights Committee, UN Doc CCPR/C/CHN-HKG/CO/4 (22 July 2022)

40. Hong Kong, China, should: (d) Ensure that the data collected through the digital applications used in the context of COVID-19 response are used strictly for specified and legitimate objectives and are deleted when such objectives have been met.

Concluding Observations on the Fifth Periodic Report of Ireland, Human Rights Committee, UN Doc CCPR/C/IRL/CO/5 (22 July 2022)

46. […] The State party should also ensure that the processing and collection of personal data are subject to effective independent oversight mechanisms and that there is access to effective remedies in cases of abuse.

Concluding Observations on the Fourth Periodic Report of Estonia, Human Rights Committee, UN Doc CCPR/C/EST/CO/4 (18 April 2019)

30. The State party should bring its regulations governing data retention and access thereto, surveillance and interception activities, and those relating to the intelligence-sharing of personal communications, into full conformity with the Covenant, in particular article 17, including with the principles of legality, proportionality and necessity. It should ensure that (a) any such interference with privacy requires prior authorization from a court or other suitable independent body and is subject to effective and independent oversight mechanisms; (b) access to communications data is limited to the extent strictly necessary for investigations into and prosecution of serious crimes; and (c) persons affected are notified of surveillance and interception activities, where possible, and have access to effective remedies in cases of abuse."

Concluding Observations on the Initial Report of Pakistan, Human Rights Committee, UN Doc CCPR/C/PAK/CO/1 (27 July 2017)

36. The State party should review its legislation on data collection and surveillance, in particular the Prevention of Electronic Crimes Act 2016, to bring it into line with its obligations under the Covenant. It should also establish independent oversight mechanisms for the implementation of the Act, including judicial review of surveillance activity; review its laws and practice of intelligence-sharing with foreign agencies to ensure its compliance with the Covenant; review all licensing requirements that impose obligations on network service providers to engage in communication surveillance, particularly in relation to indiscriminate data retention; and ensure that surveillance activities comply with the State party's obligations under the Covenant. It should further adopt a comprehensive data-protection law in line with international standards.

Concluding Observations on the Fourth Periodic Report of Switzerland, Human Rights Committee, UN Doc CCPR/C/CHE/CO/4 (27 July 2017)

46. While taking note of the human rights guarantees introduced in the Federal Act of 25 September 2016 on the Intelligence Service, the Committee is concerned that this law grants very intrusive surveillance powers to the Confederation's intelligence services on the basis of insufficiently defined objectives such as the national interest, referred to in article 3. It is also concerned that the time period for which data may be retained is not specified (art. 17).

47. The State party should take all necessary measures to guarantee that its surveillance activities are in conformity with the obligations arising from the Covenant, notably article 17. In particular, measures should be taken to ensure that the time limits for data retention are strictly regulated.

Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, UN Doc CCPR/C/ITA/CO/6 (28 March 2017)

37. The State party should review the regime regulating the interception of personal communications, hacking of digital devices and the retention of communications data with a view to ensuring (a) that such activities conform with its obligations under article 17 including with the principles of legality, proportionality and necessity, (b) that robust independent oversight systems over surveillance, interception and hacking, including by providing for judicial involvement in the authorization of such measures in all cases and affording persons affected with effective remedies in cases of abuse, including, where possible, an ex post notification that they were subject to measures of surveillance or hacking."

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/7 (17 August 2015)

24. The State Party Should: […] (d) Revise the Data Retention and Investigatory Powers Act 2014 with a view to ensuring that access to communications data is limited to the extent strictly necessary for prosecution of the most serious crimes and is dependent upon prior judicial authorization."

UN Human Rights Committee, General Comment No 16: Article 17 (Right to Privacy), UN Doc HRI/GEN/1/Rev.1 at (8 April 1988)

10. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files.

***Kaczmarek v Poland*, App No 16974/14, Judgment, European Court of Human Rights (22 February 2024)**

93. The Court notes that the surveillance material concerning the applicant in the present case was collected in the course of a security operation. The measure was applied against other people and, as submitted by the Government and confirmed by the domestic authorities, the applicant herself had not been a subject of that security operation (see paragraph 85 above). Nevertheless, the authorities had obtained material concerning her. In addition to the recording played during the press conference (see paragraph 10 above), they had also obtained transcripts of other telephone conversations which she had had with her husband and her son (see paragraph 25 above).

94. The Court further notes that the material was not destroyed but stored and included in the investigation files. The applicant applied on several occasions to have the material destroyed.

Initially, she was informed that the transcripts had become trial material and that therefore they could not be destroyed (see paragraph 26 above). Subsequently, the authorities refused to proceed with her request as, following amendments to the Code of Criminal Procedure, there were discrepancies in the interpretation of the relevant provisions concerning destruction of secret surveillance material (see paragraph 29 above). Although the applicant's request was eventually successfully submitted to the Warsaw District Court, it was dismissed on the ground that Article 238 §§ 4 and 5 of the Code of Criminal Procedure could not be applied in the applicant's case (see paragraph 32 above). The Warsaw District Court's decision, however, cannot be assessed since the reasoning was classified and has not been disclosed to the Court or to the applicant (compare *Zoltán Varga*, cited above, § 167, and *Haščák v. Slovakia*, no. 58359/12, § 96, 23 June 2022).

95. Moreover, according to the information available to the Court at the date of the adoption of the present judgment, it appears that the case files containing the transcripts of the applicant's conversations recorded in 2007 are still stored at the Warsaw Regional Prosecutor's Office. It is thus doubtful whether the relevant legal provisions, as applicable at the material time, laid down enough safeguards to protect persons in the applicant's position, who were not subject to a security operation themselves but whose conversations were nevertheless intercepted (see, *mutatis mutandis*, *Vasil Vasilev v. Bulgaria*, no. 7610/15, § 93, 16 November 2021).

96. The Court therefore concludes that the lack of sufficient clarity in the legal framework at the time of the events in the present case and the absence of procedural guarantees relating specifically to the destruction of the applicant's communications mean that the interference with the applicant's rights under Article 8 of the Convention was not "in accordance with the law". […]

***Podchasov v Russia*, App No 33696/19, Judgment, European Court of Human Rights (13 February 2024)**

50. The Court notes at the outset that the present case concerns the statutory requirement for ["Internet communications organiser" (организатор распространения информации в сети Интернет – hereinafter "ICO")] to store the content of all Internet communications and related communications data, give law-enforcement authorities or security services access to those data at their request, and decrypt electronic messages if they are encrypted.

51. As regards the storage by ICOs of Internet communications and related communications data, the Court reiterates that the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding. However, in determining whether the personal information retained by the authorities involves any of the various private-life aspects, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained (see *and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 67, ECHR 2008).

52. The Court finds that the storage by the applicant's ICO of the contents of all his Internet communications and related communications data interfered with his right to respect for his private life and correspondence (see paragraph 19 above for the domestic provisions; compare *Breyer v. Germany*, no. 50001/12, § 81, 30 January 2020, and *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, §§ 372 and 373, 11 January 2022). This storage amounts to an interference with his Article 8 rights, irrespective of whether the retained data were then accessed by the authorities. The storage, although carried out by private persons – the ICOs – is required by law; it follows that the interference is attributable to the Russian State (see *Ekimdzhiev and Others*, cited above, §§ 372 and 375).

63. […] The core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and insist on limited periods of storage (ibid., § 107).

***N.F. and Others v Russia*, Apps Nos 3537/15 and 8 others, Judgment, European Court of Human Rights (12 September 2023)**

40. With regard to the processing by the authorities of criminal-record data, the Court has indicated that it is essential to have clear, detailed rules governing the scope and application of such measures, together with minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction – thus providing sufficient guarantees against the risk of abuse and arbitrariness (see *M. v. the United Kingdom*, no. 24029/07, § 195, 13 November 2012).

***Ekimdzhiev and Ors v Bulgaria*, App No 70078/12, Judgment, European Court of Human Rights (11 January 2022)**

326. First, while those provisions specify the way in which information from the "primary recording" is to be reproduced in the "derivative data carrier" and then in any evidentiary material (see paragraphs 87 to 91 above), they say nothing about the way in which the "primary recording" and the "derivative data carrier" are to be stored. Nor do they circumscribe in any way the officials within the relevant authorities who are entitled to access them, or lay down any safeguards ensuring the integrity and confidentiality of those materials. It must be noted in this connection that since the repeal in August 2013 of point 8 of part II of Schedule no. 1 to the Protection of Classified Information Act 2002, information obtained by using special means of surveillance is no longer classified (see paragraph 102 above). It is thus apparently not subject to the rules governing the protection of such information – although the Technical Operations Agency maintained that despite the amendment both the "primary recording" obtained as a result of surveillance and the "derivative data carrier" remained classified information (see paragraph 104 above). As noted in paragraph 296 above, the internal rules to which the Government referred (see paragraphs 283 and 288 above) have not been published. They were not even disclosed in these proceedings (compare with *Big Brother Watch and Others*, cited above, 423).

327. Moreover, aside from the general rule that the content of the "derivative data carrier" must fully match that of the "primary recording" (see paragraph 89 *in fine* above), no publicly available rules exist about the way in which the "primary recording" and the "derivative data carrier" are to be examined: how the authorities are to sift through the information in them and decide which parts are relevant and are to be kept and used as evidence, and which parts are irrelevant and are to be discarded. Although the rules governing the possible use of materials obtained as a result of secret surveillance say that any such materials, including surplus information, can be used only to prevent, detect or prove serious intentional criminal offences, or to protect national security (see paragraphs 18, 84, 100 and 101 above), it is thus unclear how compliance with that limitation is ensured in practice.

328. The rules governing the destruction of the "primary recording" and the "derivative data carrier" appear sufficiently clear, although a discrepancy exists between the position in relation to materials obtained as a result of surveillance outside the framework of already pending criminal proceedings and the position in relation to materials obtained in the course of criminal proceedings: the law provides for automatic destruction and subsequent report to the judge who has authorised the surveillance in the former case, and for a report to that judge and destruction by his or her order in the latter case (see paragraphs 94 to 99 above).

329. There are, however, no special rules about the storage or destruction of the resulting evidentiary material. At least two copies of that evidentiary material are produced in each case (which appear to consist in computer files containing audio- or video-recordings – see paragraph 90 above) and of the written records which accompany them (see paragraph 91 above). The first copy is sent to the judge who has issued the surveillance warrant (ibid.). The second copy is kept first by the requesting authority and then, if criminal proceedings are opened in connection with it, it is transferred to the

case file of those proceedings – first the case file kept by the prosecuting authorities and then the case file kept by the criminal court(s) (see paragraph 92 above). It appears that both copies are stored and destroyed together with the case files of which they form part. It cannot be accepted that this provides an appropriate level of protection for information which may concern intimate aspects of someone's private life or otherwise permit a disproportionate invasion into the privacy of the people concerned or in the "correspondence" of any legal persons concerned. The scenario in which no criminal proceedings are opened also throws up many uncertainties.

330. Nor are there any publicly available rules governing the storage of information obtained through surveillance on national-security grounds – which must be kept by the relevant requesting authority for fifteen years after the end of the surveillance (see paragraph 98 above).

332. The apparent lack of clear regulation in all these fields, and of proper safeguards, makes it possible for information obtained as a result of secret surveillance to be misused for ends which have little to do with the statutory purpose.

***Eminağaoğlu v Turkey*, App No 76521/1, Judgment, European Court of Human Rights (9 March 2021)**

161. With regard to the substance of this complaint, the Court would point out that, again in the above-cited *Karabeyoğlu* case, it found that there had been a violation of Article 8 of the Convention, taking the view that the material obtained by the interception of telephone communications in criminal proceedings had been used for the purposes of the disciplinary investigation and that such interference was not "in accordance with the law" within the meaning of Article 8 § 2 of the Convention (ibid., § 119). Having assessed the present case in the light of the principles set out in its above-mentioned case-law, the Court finds that the Government have failed to present any factual element or argument that would lead to any other conclusion. Indeed, it observes in the present case that while, according to a letter of 31 December 2009, the Istanbul public prosecutor in charge of the investigation sent the applicant an information note on the discontinuance of the proceedings and the destruction of material gathered during the surveillance […], a copy undoubtedly remained in the hands of the judicial inspectors, who used this data as part of the disciplinary investigation against the applicant. As noted in the case of *Karabeyoğlu* (cited above, § 117), the use of these data outside the purpose for which they had been collected was not in conformity with domestic legislation. The Court therefore finds a violation of Article 8 of the Convention as regards the use, in the context of a disciplinary investigation, of recordings of the applicant's telephone conversations."

***Trajkovski and Chipovski v North Macedonia*, Apps Nos 53205/13 and 63320/13, Judgment, European Court of Human Rights (13 February 2020)**

51. […], it reiterates that the mere retention and storage of personal data by public authorities is to be regarded as having a direct impact on the private-life interest of the individual concerned, irrespective of whether subsequent use is made of the data […].

52. In this connection, it observes that the applicable legislation at the time did not set a specific time-limit for the retention of DNA data of the applicants as convicted persons. […] In the absence of anything to suggest that such retention may be linked to any fixed point in time, the Court considers that the respondent State permits indefinite retention period of DNA profiles.

53. […] Moreover, whereas the police are vested with the power to delete personal data from the registers (see paragraph 24 above), the law is silent on the conditions under which it can be done and procedure to be followed. Whereas the law provides, in general terms, for the possibility of judicial review coupled with a prior administrative review, there is no provision allowing for a specific review of the necessity of data retention. Similarly, there is no provision under which a person concerned can apply to have the data concerning him or her deleted if conserving the data no longer appears necessary in view of the nature of the offence, the age of the person concerned, the length

of time that has elapsed and the person's current personality (see *Gardel*, cited above, § 68).

54. In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the DNA profiles of the applicants, as persons convicted of an offence, coupled with the absence of sufficient safeguards available to the applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped the acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.

***Khadija Ismayilova v Azerbaijan*, Apps Nos 65286/13 and 57270/14, Judgment, European Court of Human Rights (10 January 2019)**

141. The storing and the release of information relating to an individual's private life come within the scope of Article 8 § 1. Public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities […].

143. The Court notes that the above information was obtained in the course of the criminal investigation. The applicant did not complain about the collection of the information, and the Court sees no issue arising under Article 8 in connection with such routine investigative steps as, for example, identifying the people who had visited the applicant's flat or questioning them as witnesses.

144. However, the public disclosure of the above-mentioned information in a press release by the Prosecutor General's Office and the Baku City Prosecutor's Office clearly constituted an interference with the applicant's right to respect for her private life.

145. In order to be justified under Article 8 § 2 of the Convention, any interference must be in accordance with the law, pursue one of the listed legitimate aims, and be necessary in a democratic society.

146. […] In the circumstances of the present case, the Court does not consider it necessary to determine whether the interference was "in accordance with the law", because in any event it lacked justification on other grounds.

147. In particular, the Government have not been able to demonstrate either a legitimate aim or the necessity for the interference in question. […] The Court considers that it would have been possible to inform the public about the nature of the investigative steps taken by the authorities (questioning of witnesses, examination of material evidence, and so on), while also at the same time respecting the applicant's privacy. The Government did not explain what legitimate aim was pursued by the publication of the address and the identity of the partner of someone who had been secretly and unlawfully filmed in the privacy of their own home when engaged in intimate acts and who had subsequently been threatened and subjected to the public dissemination of those videos.

148. The protection of the applicant's privacy was paramount in the overall context of the case, given that the criminal investigation itself, which the authorities purportedly aimed to inform the public about, had been launched in connection with the unjustified and flagrant invasion of her private life. The situation itself called for the authorities to exercise care in order not to compound further the already existing breach of the applicant's privacy.

149. Having regard to the above considerations, the Court finds that the interference was not justified.

***Catt v The United Kingdom*, App No 43514/15, Judgment, European Court of Human Rights (24 January 2019)**

119. […], in the absence of any rules setting a definitive maximum time limit on the retention of such data the applicant was entirely reliant on the diligent application of the highly flexible safeguards in the MOPI to ensure the proportionate retention of his data.

120. In this connection, the Court observes that as the applicant's personal data could potentially be retained indefinitely the only time limit that he could be certain of was that the data would held for a minimum of six years, at which point it would be subject to a scheduled review. In the present case, it is not clear that these six year reviews or any later reviews were conducted in any meaningful way. Certainly, they did not directly result in the deletion of any of the applicant's personal data.

122. Also, whilst the applicant could and did request the disclosure and destruction of his data, this safeguard appears to have been of limited impact given the refusal to delete his data or to provide any explanation for its continued retention – including the later disclosure without explanation of the retention of additional data. […]

123. Moreover, the absence of effective safeguards was of particular concern in the present case, as personal data revealing political opinions attracts a heightened level of protection […]. In this connection it notes that in the National Coordinator's statement, the definition of "domestic extremism" refers to collection of data on groups and individuals who act "outside the democratic process". Therefore, the police do not appear to have respected their own definition (fluid as it may have been in retaining data on the applicant's association with peaceful, political events: such events are a vital part of the democratic process […] Accordingly, it considers that the decisions to retain the applicant's personal data did not take into account the heightened level of protection it attracted as data revealing a political opinion, and that in the circumstances its retention must have had a "chilling effect".

124. […] The Court considers that the retention of the applicant's data in particular concerning peaceful protest has neither been shown to be absolutely necessary, nor for the purposes of a particular inquiry.

127. Accordingly, the Court is not convinced that deletion of the data would be so burdensome as to render it unreasonable. In general terms the Court would add that it would be entirely contrary to the need to protect private life under Article 8 if the Government could create a database in such a manner that the data in it could not be easily reviewed or edited, and then use this development as a justification to refuse to remove information from that database.

***Aycaguer v France*, App No 8806/12, Judgment, European Court of Human Rights (22 June 2017)**

33. The Court reiterates that the mere fact of storing data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (see *Leander v. Sweden*, 26 March 1987, § 48, Series A no. 116). The subsequent use of the stored information has no bearing on that finding (see *Amann v. Switzerland* [GC], no. 27798/95, § 69, ECHR 2000-II). As regards DNA profiles, they do contain substantial amounts of unique personal data (see *S. and Marper*, cited above, §75).

234. Furthermore, the Court observes at the outset that it fully realises that in order to protect their population as required, the national authorities can legitimately set up databases as an effective means of helping to punish and prevent certain offences, including the most serious types of crime, such as the sex offences […] (cf., in particular, *Gardel*, *B.B.* and *M.B.*, cited above, §§ 63, 62 and 54 respectively). However, such facilities cannot be implemented as part of an abusive drive to maximise the information stored in them and the length of time for which they are kept. Indeed, without respect for the requisite proportionality *vis-à-vis* the legitimate aims assigned to such mechanisms, their advantages would be outweighed by the serious breaches which they would cause to the rights and freedoms which States must guarantee under the Convention to persons under their jurisdiction (see *M.K. v. France*, no. 19522/09, § 35, 18 April 2013).

37. The Court must therefore examine whether the interference was necessary *vis-à-vis* the requirements of the Convention. Since the national authorities make the initial assessment as to where the fair balance lies in a case before a final evaluation by this Court, a certain margin of appreciation is, in principle, accorded by this Court to those authorities as regards that assessment. The breadth of this margin varies and depends on a number of factors, including the nature of the activities restricted and the aims pursued by the restrictions. Where a particularly important aspect of someone's life or identity is in issue, the State's margin of appreciation is generally narrower.

38. Personal data protection plays a primordial role in the exercise of a person's right to respect for his private life enshrined in Article 8 of the Convention. Domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of that Article. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should, in particular, ensure that such data are relevant and not excessive in relation to the purposes for which they are stored, and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. The domestic law should also comprise safeguards capable of effectively protecting the personal data recorded against inappropriate and wrongful use (see *B.B.*, cited above, § 61), while providing a practical means of lodging a request for the deletion of the data stored (see *B.B.*, cited above, § 68, and *Brunet*, cited above, §§ 41-43).

***Roman Zakharov v Russia*, App No 47143/06, Judgment, European Court of Human Rights (4 December 2015)**

251. As regards the first safeguard, both the CCrP and the OSAA provide that interceptions may be authorised by a judge for a period not exceeding six months. There is therefore a clear indication in the domestic law of the period after which an interception authorisation will expire. Secondly, the conditions under which an authorisation can be renewed are also clearly set out in law. In particular, under both the CCrP and the OSAA a judge may extend interception for a maximum of six months at a time, after a fresh examination of all the relevant materials (id.). However, as regards the third safeguard concerning the circumstances in which the interception must be discontinued, the Court notes that the requirement to discontinue interception when no longer necessary is mentioned in the CCrP only. Regrettably, the OSAA does not contain such a requirement (id.). In practice, this means that interceptions in the framework of criminal proceedings are attended by more safeguards than interceptions conducted outside such a framework, in particular in connection with "events or activities endangering national, military, economic or ecological security".

252. The Court concludes from the above that while Russian law contains clear rules on the duration and renewal of interceptions providing adequate safeguards against abuse, the OSAA provisions on discontinuation of the surveillance measures do not provide sufficient guarantees against arbitrary interference. [...]

253. Russian law stipulates that data collected as a result of secret surveillance measures constitute a State secret and are to be sealed and stored under conditions excluding any risk of unauthorised access. They may be disclosed to those State officials who genuinely need the data for the performance of their duties and have the appropriate level of security clearance. Steps must be taken to ensure that only the amount of information needed by the recipient to perform his or her duties is disclosed, and no more. The official responsible for ensuring that the data are securely stored and inaccessible to those without the necessary security clearance is clearly defined. Domestic law also sets out the conditions and procedures for communicating intercepted data containing information about a criminal offence to the prosecuting authorities. It describes, in particular, the requirements for their secure storage and the conditions for their use as evidence in criminal proceedings. The Court is satisfied that Russian law contains clear rules governing the storage, use and communication of intercepted data, making it possible to minimise the risk of

unauthorised access or disclosure.

254. As far as the destruction of intercept material is concerned, domestic law provides that intercept material must be destroyed after six months of storage, if the person concerned has not been charged with a criminal offence. If the person has been charged with a criminal offence, the trial judge must make a decision, at the end of the criminal proceedings, on the further storage and destruction of the intercept material used in evidence.

255. As regards the cases where the person concerned has not been charged with a criminal offence, the Court is not convinced by the applicant's argument that Russian law permits storage of the intercept material beyond the statutory time-limit. It appears that the provision referred to by the applicant does not apply to the specific case of storage of data collected as a result of interception of communications. The Court considers the six-month storage time-limit set out in Russian law for such data reasonable. At the same time, it deplores the lack of a requirement to destroy immediately any data that are not relevant to the purpose for which they has been obtained. The automatic storage for six months of clearly irrelevant data cannot be considered justified under Article 8.

256. Furthermore, as regards the cases where the person has been charged with a criminal offence, the Court notes with concern that Russian law allows unlimited discretion to the trial judge to store or to destroy the data used in evidence after the end of the trial. Russian law does not give citizens any indication as to the circumstances in which the intercept material may be stored after the end of the trial. The Court therefore considers that the domestic law is not sufficiently clear on this point. [...]

272. The Court notes at the outset that Order no 70 requires that the equipment installed by the communications service providers does not record or log information about interceptions. The Court has found that an obligation on the intercepting agencies to keep records of interceptions is particularly important to ensure that the supervisory body had effective access to details of surveillance activities undertaken. The prohibition on logging or recording interceptions set out in Russian law makes it impossible for the supervising authority to discover interceptions carried out without proper judicial authorisation. Combined with the law-enforcement authorities' technical ability, pursuant to the same Order no 70, to intercept directly all communications, this provision renders any supervision arrangements incapable of detecting unlawful interceptions and therefore ineffective.

***Kennedy v The United Kingdom*, App No 26839/05, Judgment, European Court of Human Rights (18 May 2010)**

162. As regards the procedure for examining, using and storing the data, the Government indicated in their submissions that, under RIPA, an intercepting agency could, in principle, listen to all intercept material collected. The Court recalls its conclusion in Liberty and Others, cited above, § 65, that the authorities' discretion to capture and listen to captured material was very wide. However, that case, unlike the present case, involved external communications, in respect of which data were captured indiscriminately. Contrary to the practice under the Interception of Communications Act 1985 concerning external communications, interception warrants for internal communications under RIPA relate to one person or one set of premises only, thereby limiting the scope of the authorities' discretion to intercept and listen to private communications. Moreover, any captured data which are not necessary for any of the authorised purposes must be destroyed.

163. As to the general safeguards which apply to the processing and communication of intercept material, the Court observes that section 15 RIPA imposes a duty on the Secretary of State to ensure that arrangements are in place to secure any data obtained from interception and contains specific provisions on communication of intercept material. Further details of the arrangements are provided by the Code. In particular, the Code strictly limits the number of persons to whom intercept material can be disclosed, imposing a requirement for the appropriate level of security clearance as well as

a requirement to communicate data only where there is a "need to know". It further clarifies that only so much of the intercept material as the individual needs to know is to be disclosed and that where a summary of the material would suffice, then only a summary should be disclosed. The Code requires intercept material, as well as copies and summaries of such material, to be handled and stored securely to minimise the risk of threat or loss. In particular, it must be inaccessible to those without the necessary security clearance. A strict procedure for security vetting is in place. In the circumstances, the Court is satisfied that the provisions on processing and communication of intercept material provide adequate safeguards for the protection of data obtained.

164. As far as the destruction of intercept material is concerned, section 15(3) RIPA requires that the intercept material and any related communications data, as well as any copies made of the material or data, must be destroyed as soon as there are no longer any grounds for retaining them as necessary on section 5(3) grounds. The Code stipulates that intercept material must be reviewed at appropriate intervals to confirm that the justification for its retention remains valid.

165. The Code also requires intercepting agencies to keep detailed records of interception warrants for which they have applied, an obligation which the Court considers is particularly important in the context of the powers and duties of the Commissioner and the IPT.

***Rotaru v Romania*, App No 28341/95, Judgment, European Court of Human Rights (4 May 2000)**

46. The Court points out that both the storing by a public authority of information relating to an individual's private life and the use of it and the refusal to allow an opportunity for it to be refuted amount to interference with the right to respect for private life secured in Article 8 § 1 of the Convention.

Commissioner for Human Rights, Council of Europe, Issue Paper on Democratic and Effective Oversight of National and Security Services, Commissioner's Recommendations (May 2015)

3. Ensure that all aspects and phases of the collection (regardless of its method of collection or provenance), processing, storage, sharing, minimisation and deletion of personal data by security services are subject to oversight by at least one institution that is external to the security services and the executive.

***NG v Direktor na Glavna direktsia 'Natsionalna politsia' pri Ministerstvo na vatreshnite raboti – Sofia* (C-118/22), Judgment, Grand Chamber, Court of Justice of the European Union (30 January 2024)**

37. In the light of the foregoing, it must be held that, by its question, the referring court asks, in essence, whether Article 4(1)(c) and (e) of Directive 2016/680, read in conjunction with Articles 5 and 10, Article 13(2)(b) and Article 16(2) and (3) thereof, and in the light of Articles 7 and 8 of the Charter, must be interpreted as precluding national legislation which provides for the storage, by police authorities, for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, of personal data, including biometric and genetic data, concerning persons who have been convicted by final judgment of an intentional criminal offence subject to public prosecution, until the death of the data subject, even in the event of his or her legal rehabilitation, without also granting that person the right to have those data erased or, where appropriate, to have their processing restricted.

42. It follows that, in particular, the collection of personal data in the context of criminal proceedings and their storage by police authorities, for the purposes set out in Article 1(1) of that directive, must, like any processing falling within the scope of that directive, comply with those requirements. Such storage also constitutes an interference with the fundamental rights to respect for private life and to

the protection of personal data, irrespective of whether or not the information stored is sensitive, whether or not the persons concerned have been inconvenienced in any way on account of that interference, or whether or not the stored data will subsequently be used (see, by analogy, judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C 140/20, EU:C:2022:258, paragraph 44 and the case-law cited).

44. In that context, Article 5 of that directive requires the Member States to provide for the establishment of appropriate time limits for the erasure of personal data or for a periodic review of the need for the storage of those data and procedural measures to ensure that those time limits are observed.

***Draft Agreement between Canada and the European Union on the Transfer of Passenger Name Record data (1/15)*, Court of Justice of the European Union, Grand Chamber, Opinion pursuant to Article 218(11) TFEU (26 July 2017)**

190. In order to ensure that the retention of the PNR data transferred, the access to that data by the Canadian authorities referred to in the envisaged agreement and the use of that data by those authorities is limited to what is strictly necessary, the envisaged agreement should, in accordance with the settled case-law of the Court [...], lay down clear and precise rules indicating in what circumstances and under which conditions those authorities may retain, have access to and use such data.

191. So far as the retention of personal data is concerned, it must be pointed out that the legislation in question must, inter alia, continue to satisfy objective criteria that establish a connection between the personal data to be retained and the objective pursued.

192. As regards the use, by an authority, of legitimately retained personal data, it should be recalled that the Court has held that EU legislation cannot be limited to requiring that access to such data should be for one of the objectives pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use.

202. […] it is essential that the use of retained PNR data, during the air passengers' stay in Canada, should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court, or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by the competent authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime.

205. As regards air passengers in respect of whom no such risk has been identified on their arrival in Canada and up to their departure from that non-member country, there would not appear to be, once they have left, a connection — even a merely indirect connection — between their PNR data and the objective pursued by the envisaged agreement which would justify that data being retained. The considerations put forward before the Court, inter alia, by the Council and the Commission regarding the average lifespan of international serious crime networks and the duration and complexity of investigations relating to those networks, do not justify the continued storage of the PNR data of all air passengers after their departure from Canada for the purposes of possibly accessing that data, regardless of whether there is any link with combating terrorism and serious transnational crime.

206. The continued storage of the PNR data of all air passengers after their departure from Canada is not therefore limited to what is strictly necessary. [...]

210. Lastly, in so far as Article 9(2) of the envisaged agreement, which provides that Canada is to hold PNR data 'in a secure physical environment that is protected with access controls', means that that data has to be held in Canada, and in so far as Article 16(6) of that agreement, under which Canada is to destroy the PNR data at the end of the PNR data retention period, must be understood as requiring the irreversible destruction of that data, those provisions may be regarded as meeting

the requirements as to clarity and precision.

***Patrick Breyer Bundesrepublik Deutschland* (C-582/14), Judgment, Court of Justice of the European Union (19 October 2016)**

33. As a preliminary point, it must be noted that, in paragraph 51 of the Judgment of 24 November 2011 [...] the Court held essentially that the IP addresses of internet users were protected personal data because they allow users to be precisely identified.

34. However, that finding by the Court related to the situation in which the collection and identification of the IP addresses of internet users is carried out by internet service providers.

35. In the present case, the first question concerns the situation in which it is the online media services provider, namely the Federal Republic of Germany, which registers IP addresses of the users of a website that it makes accessible to the public, without having the additional data necessary in order to identify those users.

36. Furthermore, it is common ground that the IP addresses to which the national court refers are 'dynamic' IP addresses, that is to say provisional addresses which are assigned for each internet connection and replaced when subsequent connections are made, and not 'static' IP addresses, which are invariable and allow continuous identification of the device connected to the network [...]

38. It must be noted, first of all, that it is common ground that a dynamic IP address does not constitute information relating to an 'identified natural person', since such an address does not directly reveal the identity of the natural person who owns the computer from which a website was accessed, or that of another person who might use that computer [...]

40. In that connection, it is clear from the wording of Article 2(a) of Directive 95/46 that an identifiable person is one who can be identified, directly or indirectly.

41. The use by the EU legislature of the word 'indirectly' suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified [...]

43. In so far as that recital refers to the means likely reasonably to be used by both the controller and by 'any other person', its wording suggests that, for information to be treated as 'personal data' within the meaning of Article 2(a) of that directive, it is not required that all the information enabling the identification of the data subject must be in the hands of one person [...]

45. However, it must be determined whether the possibility to combine a dynamic IP address with the additional data held by the internet service provider constitutes a means likely reasonably to be used to identify the data subject […]

47. Although the referring court states in its order for reference that German law does not allow the internet service provider to transmit directly to the online media services provider the additional data necessary for the identification of the data subject, it seems however, subject to verifications to be made in that regard by the referring court that, in particular, in the event of cyber-attacks legal channels exist so that the online media services provider is able to contact the competent authority, so that the latter can take the steps necessary to obtain that information from the internet service provider and to bring criminal proceedings.

48. Thus, it appears that the online media services provider has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority and the internet service provider, on the basis of the IP addresses stored.

49. Having regard to all the foregoing considerations, the answer to the first question is that Article 2(a) of Directive 95/46 must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person. […]

62. Article 7(f) of that directive precludes Member States from excluding, categorically and in general, the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in a particular case. Thus, Member States cannot definitively prescribe, for certain categories of personal data, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case.

63. As regards the processing of personal data of the users of online media websites, legislation, such as that at issue in the main proceedings, reduces the scope of the principle laid down in Article 7(f) of Directive 95/46 by excluding the possibility to balance the objective of ensuring the general operability of the online media against the interests or fundamental rights and freedoms of those users which, in accordance with that provision, calls for protection under Article 1(1) of that directive.

64. It follows from all of the foregoing considerations that the answer to the second question is that Article 7(f) of Directive 95/46 must be interpreted as meaning that it precludes the legislation of a Member State under which an online media services provider may collect and use personal data relating to a user of those service, without his consent, only in so far as the collection and use of that information are necessary to facilitate and charge for the specific use of those services by that user, even though the objective aiming to ensure the general operability of those services may justify the use of those data after consultation of those websites.

V. TRANSPARENCY REQUIREMENTS

UN Human Rights Council Resolution on New and Emerging Digital Technologies and Human Rights, UN Doc A/HRC/RES/53/29 (14 July 2023)

3. *Highlights* the importance of the need to respect, protect and promote human rights and fundamental freedoms, in recognition of the inherent dignity of the human person, throughout the lifecycle of artificial intelligence systems and, towards this end, the need to pay particular attention to: (c) Promoting the transparency of artificial intelligence systems and adequate explainability of artificial intelligence-supported decisions, taking into account the various levels of human rights risks arising from these technologies;

Report of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/48/31 (13 September 2021)

56. Promoting transparency should go further by including sustained efforts to overcome the "black box" problem […]. The development and systematic deployment of methodologies to make AI systems more explainable – often referred to as algorithmic transparency – is of utmost importance for ensuring adequate rights protections. This is most essential when AI is used to determine critical issues within judicial processes or relating to social services that are essential for the realization of economic, social and cultural rights. Researchers have already developed a range of approaches that further that goal, and increased investments in this area are essential. States should also take steps to ensure that intellectual property protections do not prevent meaningful scrutiny of AI systems that have human rights impacts. Procurement rules should be updated to reflect the need for transparency, including auditability of AI systems. In particular,

States should avoid using AI systems that can have material adverse human rights impacts but cannot be subject to meaningful auditing. […]

60. The High Commissioner recommends that States and business enterprises: (b) Dramatically increase the transparency of their use of AI, including by adequately informing the public and affected individuals and enabling independent and external auditing of automated systems. The more likely and serious the potential or actual human rights impacts linked to the use of AI are, the more transparency is needed; […]

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

41. State authorities and oversight bodies should also engage in public information about the existing laws, policies and practices in surveillance and communications interception and other forms of processing of personal data, open debate and scrutiny being essential to understanding the advantages and limitations of surveillance techniques (see A/HRC/13/37, para. 55). Those who have been the subject of surveillance should be notified and have explained to them ex post facto the interference with their right to privacy. They also should be entitled to alter and/or delete irrelevant personal information, provided that information is not needed any longer to carry out any current or pending investigation (see A/HRC/34/60, para. 38).

Committee on the Elimination of Racial Discrimination, General Recommendation No 36 (2020) on Preventing and Combating Racial Profiling by Law Enforcement Officials, UN Doc CERD/C/GC/36 (17 December 2020)

61. States should take all appropriate measures to ensure transparency in the use of algorithmic profiling systems. This includes public disclosure of the use of such systems and meaningful explanations of the ways in which the systems work, the data sets that are being used, and the measures in place to prevent or mitigate human rights harms.

Concluding Observations on the Seventh Periodic Report of Sweden, Human Rights Committee, UN Doc CCPR/C/SWE/CO/7 (28 April 2016)

36. While acknowledging the number of safeguards in place to prevent abuse in the application of the Signals Intelligence Act, the Committee remains concerned about the limited degree of transparency with regard to the scope of such surveillance powers and the safeguards on their application [...]

37. The State party should increase the transparency of the powers of and safeguards on the National Defence Radio Establishment, the Foreign Intelligence Court and the Data Inspection Board, by considering to make their policy guidelines and decisions public, in full or in part, subject to national security considerations and the privacy interests of individuals concerned by those decisions [...]

Annual Report of the Inter-American Commission on Human Rights 2020, Volume II – Annual Report of the Office of the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II Doc 28 (30 March 2021)

58. In short, the obstacles to access to public information and the persistent lack of transparency surrounding the surveillance activities of the States of the Americas are often barriers to accountability for their lawful use, which should follow the requirements of prior judicial

authorization and be strictly necessary and proportionate to the legitimate interests the State seeks to protect. […]

117. When the State takes initiatives to guarantee national security and prevent or counteract other threats, it must ensure that individuals are, at a minimum, adequately informed about the legal framework for surveillance and its purpose, as well as the regulatory framework of surveillance programs; the procedures to be followed for authorization, the selection of targets and the use or handling of data; the protocols for the sharing, storage and destruction of intercepted material, as well as the entities authorized to carry out surveillance actions and statistics on the use of these actions, and the bodies responsible for implementing and monitoring such programs.

118. While the protection of national security may justify the use of surveillance in private communications, it must be subject to a series of requirements and guarantees, applied in a strictly proportional and necessary manner. In the digital age, surveillance can be a particularly invasive act, seriously affecting the right to privacy, freedom of thought and expression, and the procedural rights of individuals who have been or believe themselves to be targeted for surveillance, as well as journalists, human rights defenders, and whistleblowers […].

119. The Tshwane Principles propose that States guarantee certain minimum standards of transparency about this increasingly invasive and widespread activity in the digital age. Therefore, States must ensure that people are informed about: i) the laws governing all forms of surveillance, both covert and overt, including indirect surveillance such as profiling and data-mining; ii) the permissible objectives of surveillance; (iii) the threshold of suspicion required to initiate or continue surveillance, as well as the procedures for authorizing and reviewing the use of such measures; iii) the types of personal data that may be collected and/or processed for national security purposes and the criteria that apply to the use, retention, deletion, and transfer of these data; and iv) the entities authorized to conduct surveillance, and statistics about the use of such surveillance. The State must ensure that society is informed of all unlawful surveillance.

120. States should, at the very least, publicly disclose information about the regulatory framework of surveillance programs; the entities in charge of their implementation and oversight; the procedures for authorizing, choosing targets, and using the data collected; and the use of these techniques, including aggregate information on their scope. The State must ensure program transparency and accountability and should allow service providers to provide aggregate data on the number and scope of device access requests they receive.

In view of the region's ongoing challenges that have been highlighted in this report, the Office of the Special Rapporteur for Freedom of Expression makes the following recommendations to the member states of the OAS:

(7) In implementing measures to strengthen the right of access to information and the protection of human rights, states should consider that there is a compelling public interest in the disclosure of information that helps ensure the transparency of the framework, conditions, and outcomes of state surveillance activities, in a manner consistent with international standards. Certain categories of information that allow citizens to have knowledge of the State's actions in this field, and to prevent and detect abuses, should be disclosed when requested—without revealing the targets of the surveillance—or published when it comes to procurement and spending on surveillance technology.

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

5. *Encourages* all States to promote an open, secure, stable, accessible and peaceful information and communications technology environment based on respect for international law, including the obligations enshrined in the Charter of the United Nations and human rights instruments;

7. *Calls upon* all States: (e) To establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data;

** See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014)*

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

50. To be compliant with those standards, national laws must: (d) Require, given the extreme risks of abuse associated with targeted surveillance technologies, that authorized uses be subjected to detailed record-keeping requirements. Surveillance requests should only be permitted in accordance with regular, documented legal processes and the issuance of warrants for such use. Surveillance subjects should be notified of the decision to authorize their surveillance as soon as such a notification would not seriously jeopardize the purpose of the surveillance.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014)

39. A public legislative process provides an opportunity for Governments to justify mass surveillance measures to the public. Open debate enables the public to appreciate the balance that is being struck between privacy and security. A transparent law-making process should also identify the vulnerabilities inherent in digital communications systems, enabling users to make informed choices. This is not only a core ingredient of the requirement for legal certainty under article 17 of the Covenant; it is also a valuable means of ensuring effective public participation in a debate on a matter of national and international public interest [...]

40. By contrast, the use of delegated legislation (instruments enacted by the executive under delegated powers) has already permitted the adoption of secret legal frameworks for mass surveillance, inhibiting the ability of the legislature, the judiciary and the public to scrutinize the use of these new powers. Such provisions do not meet the quality of law requirements in article 17 of the Covenant because they are not sufficiently accessible to the public. While there may be legitimate public interest reasons for maintaining the secrecy of technical and operational specifications, these do not justify withholding from the public generic information about the nature and extent of a State's Internet penetration. Without such information, it is impossible to assess the legality, necessity and proportionality of these measures. States should therefore be transparent about the use and scope of mass communications surveillance (see A/HRC/23/40, para. 91). [...]

63. States should be transparent about the nature and extent of their Internet penetration, its methodology and its justification, and should provide a detailed public account of the tangible benefits that accrue from its use.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, UN Doc A/HRC/23/40 (17 April 2013)

91. States should be completely transparent about the use and scope of communications surveillance techniques and powers. They should publish, at minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation and purpose.

92. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc A/HRC/13/37 (28 December 2009)

54. The application of secrecy privileges for surveillance systems inhibits the ability of legislatures, judicial bodies and the public to scrutinize State powers. [...]

55. The principle of transparency and integrity requires openness and communication about surveillance practices. [...]

56. Open debate and scrutiny is essential to understanding the advantages and limitations of surveillance techniques, so that the public may develop an understanding of the necessity and lawfulness of surveillance. In many States, parliaments and independent bodies have been charged with conducting reviews of surveillance policies and procedures, and on occasion have been offered the opportunity for pre-legislative review. This has been aided by the use of sunset and review clauses in legislation.

Concluding Observations on the Sixth Periodic Report of Hungary, Human Rights Committee, UN Doc CCPR/C/HUN/CO/6 (9 May 2018)

44. The State party should increase the transparency of the powers of the legal framework on secret surveillance for national security purposes (section 7/E (3) surveillance) […]

Concluding Observations on the Initial Report of South Africa, Human Rights Committee, UN Doc CCPR/C/ZAF/CO/1 (27 April 2016)

43. The State party should increase the transparency of its surveillance policy.

Annual Report of the Inter-American Commission on Human Rights 2019, Volume II – Annual Report of the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II. Doc 5 (24 February 2020)

25. […] the Office of the Special Rapporteur recommends Member States to: B. Ensure that the public can have access to information on programs for surveillance of private communications, their scope and the existing controls to guarantee that they cannot be used arbitrarily. In any case, States must establish independent control mechanisms to ensure the transparency and accountability of these programs.

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet OEA/Ser.L/V/II. CIDH/RELE/INF.11/13 (31 December 2013)

166. The State must be transparent with respect to the laws regulating communications surveillance and the criteria used for their application. The principle of "maximum disclosure" is applicable to this

issue, and indeed governs all State acts: they are public and can only be kept secret from the public under the strictest circumstances, provided that this confidentiality is established by law, seeks to fulfil a legitimate aim under the American Convention, and is necessary in a democratic society.

167. As the European Court of Human Rights has held, a secret surveillance system can "undermine or even destroy democracy under the cloak of defending it." The Court therefore demands that there be "adequate and effective guarantees against abuse." To determine whether this is being done in a particular case, the Court indicated that it is necessary to examine "nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law."

168. States should disclose general information on the number of requests for interception and surveillance that have been approved and rejected, and should include as much information as possible, such as—for example—a breakdown of requests by service provider, type of investigation, time period covered by the investigations, etc.

169. The service providers should be able to publicly disclose the procedures they use when they receive requests for information from government authorities, as well as information on at least the types of requests they receive and the number of requests. On this point, it bears noting that various internet companies have adopted the practice of issuing transparency reports that disclose some aspects of the government requests for access to user information they receive.

VI. SAFEGUARDS IN INTELLIGENCE SHARING AND DATA TRANSFERS

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

Emphasizing that States must respect international human rights obligations regarding the right to privacy when they intercept digital communications of individuals and/or collect personal data, when they share or otherwise provide access to data collected through, inter alia, information- and intelligence-sharing agreements and when they require disclosure of personal data from third parties, including business enterprises,

** See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014)*

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)

8. *Calls upon* States: (d) To respect international human rights obligations, including the right to privacy, when States intercept digital communications of individuals and/or collect personal data, when they share or otherwise provide access to data collected through, inter alia, information- and intelligence-sharing agreements and when they require disclosure of personal data from third parties, including business enterprises;

Report of the United Nations High Commissioner for Human Rights, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests, UN Doc A/HRC/44/24 (24 June 2020)

53. In this context, the High Commissioner recommends that States: (d) Ensure that any interference with the right to privacy, including by communications surveillance and intelligence-sharing, complies with international human rights law, including the principles of legality, necessity and proportionality;

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

21. Governments across the globe routinely share intelligence on individuals outside any legal framework and without adequate oversight. Intelligence-sharing poses the serious risk that a State may use this approach to circumvent domestic legal constraints by relying on others to obtain and then share information. Such a practice would fail the test of lawfulness and may undermine the essence of the right to privacy (see A/HRC/27/37, para. 30). The threat to human rights protections is particularly acute where intelligence is shared with States with weak rule of law and/or a history of systematically violating human rights. Intelligence received by one State from another may have been obtained in violation of international law, including through torture and other cruel, inhuman or degrading treatment. The human rights risks posed by intelligence-sharing are heightened by the current lack of transparency, accountability and oversight of intelligence-sharing arrangements (see A/69/397, para. 44, CCPR/C/GBR/CO/7, para. 24, and CCPR/C/SWE/CO/7, para. 36). …

37. Powers of secret surveillance can only be justified as far as they are strictly necessary for achieving a legitimate aim and meet the proportionality requirement (see A/HRC/23/40, para. 83 (b)). Secret surveillance measures must be limited to preventing or investigating the most serious crimes or threats. The duration of the surveillance should be limited to the strict minimum necessary for achieving the specified goal. There must be rigorous rules for using and storing the data obtained and the circumstances in which the data collected and stored must be erased need to be clearly defined, based on strict necessity and proportionality. Intelligence-sharing must be subject to the same principles of legality, strict necessity and proportionality.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014)

44. The absence of laws to regulate information-sharing agreements between States has left the way open for intelligence agencies to enter into classified bilateral and multilateral arrangements that are beyond the supervision of any independent authority. Information concerning an individual's communications may be shared with foreign intelligence agencies without the protection of any publicly accessible legal framework and without adequate (or any) safeguards. […] Such practices make the operation of the surveillance regime unforeseeable for those affected by it and are therefore incompatible with article 17 of the Covenant.

Concluding Observations on the Seventh Periodic Report of Sweden, Human Rights Committee, UN Doc CCPR/C/SWE/CO/7 (28 April 2016)

36. [The Committee is] concerned about the lack of sufficient safeguards against arbitrary interference with the right to privacy with regard to the sharing of raw data with other intelligence agencies.

37. The State party should increase the transparency of the powers of and safeguards on the

National Defence Radio Establishment, the Foreign Intelligence Court and the Data Inspection Board, by considering to make their policy guidelines and decisions public, in full or in part, subject to national security considerations and the privacy interests of individuals concerned by those decisions. It should ensure: (a) that all laws and policies regulating the intelligence-sharing of personal data are in full conformity with its obligations under the Covenant, in particular article 17, including the principles of legality, proportionality and necessity; (b) that effective and independent oversight mechanisms over intelligence-sharing of personal data are put in place; and (c) that affected persons have proper access to effective remedies in cases of abuse.

***Draft Agreement between Canada and the European Union on the Transfer of Passenger Name Record data* (1/15), Court of Justice of the European Union, Grand Chamber, Opinion pursuant to Article 218(11) TFEU (26 July 2017)**

124. […] the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental right […], whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities. In this connection, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference.

125. Consequently, both the transfer of PNR data from the European Union to the Canadian Competent Authority and the framework negotiated by the European Union with Canada of the conditions concerning the retention of that data, its use and its subsequent transfer to other Canadian authorities, Europol, Eurojust, judicial or police authorities of the Member States or indeed to authorities of third countries, [...] constitute interferences with the right. [...]

141. In order to satisfy [the principle of proportionality], the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing. Those considerations apply particularly where the protection of the particular category of personal data that is sensitive data is at stake. […]

168. [...] the PNR data transferred to Canada is mainly intended to be subject to analyses by automated means, based on pre-established models and criteria and on cross-checking with various databases.

169. the assessment of the risks to public security presented by air passengers is carried out [...] by means of automated analyses of the PNR data before the arrival of those air passengers in Canada. Since those analyses are carried out on the basis of unverified personal data and are based on pre-established models and criteria, they necessarily present some margin of error, as, inter alia, the French Government and the Commission conceded at the hearing. [...]

171. It is true that, as regards the consequences of the automated processing of PNR data, Article 15 of the envisaged agreement provides that Canada is not to take 'any decisions significantly adversely affecting a passenger solely on the basis of automated processing of PNR data'. [...]

172. That being so, the extent of the interference which automated analyses of PNR data entail in respect of the rights enshrined in Articles 7 and 8 of the Charter essentially depends on the pre-established models and criteria and on the databases on which that type of data processing

is based... the pre-established models and criteria should be specific and reliable, making it possible [...] to arrive at results targeting individuals who might be under a 'reasonable suspicion' of participation in terrorist offences or serious transnational crime and should be non-discriminatory. Similarly, it should be stated that the databases with which the PNR data is cross-checked must be reliable, up to date and limited to databases used by Canada in relation to the fight against terrorism and serious transnational crime.

173. Furthermore, since the automated analyses of PNR data necessarily involve some margin of error [...] any positive result obtained following the automated processing of that data must [...] be subject to an individual re-examination by non-automated means before an individual measure adversely affecting the air passengers concerned is adopted. Consequently, such a measure may not [...] be based solely and decisively on the result of automated processing of PNR data.

174. Lastly, in order to ensure that, in practice, the pre-established models and criteria, the use that is made of them and the databases used are not discriminatory and are limited to that which is strictly necessary, the reliability and topicality of those pre-established models and criteria and databases used should, taking account of statistical data and results of international research, be covered by the joint review of the implementation of the envisaged agreement […]

214. In this connection, it must be recalled that a transfer of personal data from the European Union to a non-member country may take place only if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union. That same requirement applies in the case of the disclosure of PNR data by Canada to third countries [...] in order to prevent the level of protection provided for in that agreement from being circumvented by transfers of personal data to third countries and to ensure the continuity of the level of protection afforded by EU law […]

216. Article 12(3) of the envisaged agreement allows Canada to 'make any disclosure of information subject to reasonable legal requirements and limitations ... with due regard for the legitimate interests of the individual concerned'. However, that agreement does not delimit the nature of the information that may be disclosed, nor the persons to whom such disclosure may be made, nor even the use that is to be made of that information.

217. Moreover, the envisaged agreement does not define the terms 'legal requirements and limitations' or the terms 'legitimate interests of the individual concerned', nor does it require that the disclosure of PNR data to an individual be linked to combating terrorism and serious transnational crime or that the disclosure be conditional on the authorisation of a judicial authority or an independent administrative body. In those circumstances, that provision exceeds the limits of what is strictly necessary.

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019)

Emphasizing also that States must respect international human rights obligations regarding the right to privacy when they intercept digital communications of individuals and/or collect personal data, when they share or otherwise provide access to data collected through, inter alia, intelligence-sharing agreements, and when they require disclosure of personal data from third parties, including business enterprises,

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

30. The requirement of accessibility is also relevant when assessing the emerging practice of States to outsource surveillance tasks to others. There is credible information to suggest that some Governments systematically have routed data collection and analytical tasks through jurisdictions with weaker safeguards for privacy. Reportedly, some Governments have operated a transnational network of intelligence agencies through interlocking legal loopholes, involving the coordination of surveillance practice to outflank the protections provided by domestic legal regimes. Such practice arguably fails the test of lawfulness because [...] it makes operation of the surveillance regime unforeseeable for those affected by it. It may undermine the essence of the right protected by Article 17 of the International Covenant on Civil and Political Rights... States have also failed to take effective measures to protect individuals within their jurisdiction against illegal surveillance practices by other States or business entities, in breach of their own human rights obligations.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights while Counter-Terrorism, Human Rights Implications of the Development, Use, Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism, UN Doc A/HRC/52/39 (1 March 2023)

50. […] Finally, she stresses that it is urgent that a human rights-compliant review of intelligence cooperation be undertaken, which will require consistent screening of transferred intelligence by methods such as data-sharing alerts to oversight bodies, consistent review of log files, deletion monitoring and a moratorium on intelligence-sharing with comparator agencies that have been identified as engaged in a consistent pattern of human rights violations.

Report of the Working Group on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination, Impact of the Use of Private Military and Security Services in Immigration and Border Management on the Protection of the Rights of All Migrants, UN Doc A/HRC/45/9 (9 July 2020)

40. […] Companies have developed platforms that enable users to search across databases, allowing them to cross-reference data collected for different purposes. This push towards interoperability carries risks, for example, due to greater interactions between law enforcement and immigration databases. Among other things, immigration authorities have allegedly used this information to track, detain and deport migrants, including children.

42. […] It not only enables the transmission of real-time information on the movement of people and vessels along coastal and land borders, but often penetrates into border regions and further afield. This information is shared among border, security and other authorities within the same country, and increasingly between States. […]"

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/40/63 (16 October 2019)

31. The Special Rapporteur supports the strict application of the tests of proportionality and necessity in a democratic society as an important benchmark with global repercussions. The intelligence agencies in other regions may be influenced by the increasingly strict standards applied in Europe. Intelligence analysis containing personal information and other personal data transferred from and to Europe thus needs to come under correspondingly strict oversight to ensure that these privacy-respectful standards are upheld in Europe and serve as a possible good practice and model worldwide.

32. […] A number of new technologies, in particular the Internet, smartphones, big data analytics, wearables, smart energy and smart cities, render individuals and communities more vulnerable to government surveillance of corporations in their countries, as well as by the intelligence agencies of foreign States and corporations.

48. […] in relation to any personal information exchanged between intelligence services and law enforcement agencies within a country, and across borders;

(a) All UN Member States should amend their laws to empower their independent authorities entrusted with oversight of intelligence activities, to specifically and explicitly, oversight of all personal information exchanged between the intelligence agencies of the countries for which they are responsible.

(b) Whenever possible and appropriate, the independent oversight authorities of both the transmitting and the receiving States should have immediate and automated access to the personal data exchanged between the intelligence services and/or law enforcement agencies of their respective States;

(c) All UN Member States should amend their legislation to specifically empower their national and state Intelligence Oversight Authorities to have the legal authority to share information, consult and discuss best oversight practices with the Oversight Authorities of those States to which personal data has been transmitted or otherwise exchanged by the intelligence agencies of their respective States;

(d) When an intelligence agency transmits intelligence analysis containing personal information or other forms of personal data received from another State to a third State or group of States, this latter exchange should be subject to those States' intelligence oversight authorities.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/23/40 (17 April 2013)

86. […] At the international level, States should enact Mutual Legal Assistance Treaties to regulate access to communications data held by foreign corporate actors.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc A/HRC/13/37 (28 December 2009)

50. Whereas data protection law should protect information collected for one purpose being used for another, national security and law enforcement policies are generally exempted from these restrictions... The Special Rapporteur is concerned that this limits the effectiveness of necessary safeguards against abuse. States must be obliged to provide a legal basis for the reuse of information, in accordance with constitutional and human rights principles. This must be done within the human rights framework, rather than resorting to derogations and exemptions. This is particularly important when information is shared across borders; furthermore, when information is shared between States, protections and safeguards must continue to apply.

Concluding Observations on the Eighth Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/8 (26 March 2024)

51. […] [The State Party] should ensure that its regulations relating to the intelligence-sharing of personal communications are in full conformity with the Covenant, in particular article 17,

Concluding Observations on the Fourth Periodic Report of Estonia, Human Rights Committee, UN Doc CCPR/C/EST/CO/4 (18 April 2019)

29. […] The Committee is also concerned about the lack of sufficient safeguards against arbitrary interference with the right to privacy with regard to surveillance and interception activities by State security and intelligence agencies and with regard to intelligence sharing with foreign entities (art.

17).

30. The State party should bring its regulations governing data retention and access thereto, surveillance and interception activities, and those relating to the intelligence-sharing of personal communications, into full conformity with the Covenant, in particular article 17, including with the principles of legality, proportionality and necessity. It should ensure that (a) any such interference with privacy requires prior authorization from a court or other suitable independent body and is subject to effective and independent oversight mechanisms; (b) access to communications data is limited to the extent strictly necessary for investigations into and prosecution of serious crimes; and (c) persons affected are notified of surveillance and interception activities, where possible, and have access to effective remedies in cases of abuse.

Concluding Observations on the Initial Report of Pakistan, Human Rights Committee, UN Doc CCPR/C/PAK/CO/1 (27 July 2017)

35. While noting the State party's view that the Prevention of Electronic Crimes Act 2016 complies with the Convention on Cybercrime, the Committee is concerned that the Act provides for [...] (d) the sharing of information and cooperation with foreign governments without judicial authorization or oversight (arts. 17 and 19).

36. The State party should review its legislation on data collection and surveillance, in particular, the Prevention of Electronic Crimes Act 2016, to bring it in line with its obligations under the Covenant. It should […] review its laws and practice of intelligence sharing with foreign agencies to ensure its compliance with the Covenant. [...]

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/7 (17 August 2015)

24. The State Party should: […] (c) Ensure that robust oversight systems over surveillance, interception and intelligence-sharing of personal communications activities are in place, including by providing for judicial involvement in the authorization of such measures in all cases, and by considering the establishment of strong and independent oversight mandates with a view to preventing abuses.

Concluding Observations on the Sixth Periodic Report of Canada, Human Rights Committee, UN Doc CCPR/C/CAN/CO/6 (13 August 2015)

10. Bill C-51 creates under the security of Canada Information Sharing Act, an increased sharing of information among federal government agencies on the basis of a very broad definition of activities that undermine the security of Canada which does not fully prevent that inaccurate or irrelevant information is shared [...] The State Party should […] (c) Provide adequate safeguards to ensure that information-sharing under the Security of Canada Information Sharing Act does not result in human rights abuses. […]

Commissioner for Human Rights, Council of Europe, Positions on Counter-Terrorism and Human Rights Protection, CommDH/PositionPaper(2015)1 (5 June 2015)

The principle of making data available to other authorities should not be used to circumvent European and national constitutional data-protection standards.

***Big Brother Watch and Others v The United Kingdom*, Apps Nos 58170/13, 62322/14 and 24960/15, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

362. Despite being one of the six *Weber* criteria, to date the Court has not yet provided specific

guidance regarding the precautions to be taken when communicating intercept material to other parties. However, it is now clear that some States are regularly sharing material with their intelligence partners and even, in some instances, allowing those intelligence partners direct access to their own systems. Consequently, the Court considers that the transmission by a Contracting State to foreign States or international organisations of material obtained by bulk interception should be limited to such material as has been collected and stored in a Convention compliant manner and should be subject to certain additional specific safeguards pertaining to the transfer itself. First of all, the circumstances in which such a transfer may take place must be set out clearly in domestic law. Secondly, the transferring State must ensure that the receiving State, in handling the data, has in place safeguards capable of preventing abuse and disproportionate interference. In particular, the receiving State must guarantee the secure storage of the material and restrict its onward disclosure. This does not necessarily mean that the receiving State must have comparable protection to that of the transferring State; nor does it necessarily require that an assurance is given prior to every transfer. Thirdly, heightened safeguards will be necessary when it is clear that material requiring special confidentiality – such as confidential journalistic material – is being transferred. Finally, the Court considers that the transfer of material to foreign intelligence partners should also be subject to independent control.

***Centrum för Rättvisa v Sweden*, App No 35252/08, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

322. The Court observes that the possibility for the FRA to share intelligence it has obtained with foreign partners is provided for in Swedish law, which also sets out the relevant general purpose (see paragraphs 49 and 74 above). It is to be observed, however, that the level of generality of the terms used cannot but lead to the conclusion that the FRA may send intelligence abroad whenever this is considered to be in the national interest.

323. Having regard to the unpredictability of situations that may warrant cooperation with foreign intelligence partners, it is understandable that the precise scope of intelligence sharing cannot be circumscribed in law through, for example, exhaustive and detailed lists of such situations or the types of intelligence or content that can be transmitted. The applicable legal regulation and practice must operate, however, in a manner capable of limiting the risk of abuse and disproportionate interference with Article 8 rights.

324. […] Therefore, the safeguards internally applicable in Sweden in the process of obtaining the intelligence that may later be transmitted to a foreign partner also limit, at least to a certain extent, the risk of adverse consequences that may ensue after the transmission has taken place.

325. The Court also notes that the supervision mechanisms provided for under the Personal Data Processing Act, specifically tailored to the protection of personal data, apply to all activities of the FRA (see paragraphs 56 above).

326. In the Court's view, despite the above considerations, the absence, in the relevant signals intelligence legislation, of an express legal requirement for the FRA to assess the necessity and proportionality of intelligence sharing for its possible impact on Article 8 rights is a substantial shortcoming of the Swedish regime of bulk interception activities. It appears that, as a result of this state of the law, the FRA is not obliged to take any action even in situations when, for example, information seriously compromising privacy rights is present in material to be transmitted abroad without its transmission being of any significant intelligence value. Furthermore, despite the fact that the Swedish authorities obviously lose control over the shared material once it has been sent out, no legally binding obligation is imposed on the FRA to analyse and determine whether the foreign recipient of intelligence offers an acceptable minimum level of safeguards (see paragraph 276 above).

330. […] the absence of a requirement in the Signals Intelligence Act or other relevant legislation

that consideration be given to the privacy interests of the individual concerned when making a decision about intelligence sharing is a significant shortcoming of the Swedish regime, to be taken into account in the Court's assessment of its compatibility with Article 8 of the Convention.

***Szabó and Vissy v Hungary*, App No 37138/14, Judgment, European Court of Human Rights (12 January 2016)**

78. The governments' more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance – a practice, whose usefulness in combating international terrorism is, once again, not open to question and which concerns both exchanges between Member States of the Council of Europe and with other jurisdictions – is yet another factor in requiring particular attention when it comes to external supervision and remedial measures.

***Ligue des droits humains v Conseil des ministres* (C-817/19), Judgment, Grand Chamber, Court of Justice of the European Union (21 June 2022)**

222 It is true that, where a request for the subsequent disclosure and assessment of PNR data is introduced before the expiry of the period of six months after the transfer of those data, Article 6(2)(b) of the PNR Directive does not expressly provide for such a procedural requirement. Nonetheless, the interpretation of the latter provision must take into consideration recital 25 of that directive, from which it is apparent that, by laying down the said procedural requirement, the EU legislature intended 'to ensure the highest level of data protection' concerning access to PNR data in a form which permits direct identification of the data subject. Any request for subsequent disclosure and assessment implies such access to those data, irrespective of whether that request is introduced before the expiry of the period of six months after the transfer of the PNR data to the PIU or whether it is introduced after the expiry of that period.

***Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems* (C-311/18), Judgment, Grand Chamber, Court of Justice of the European Union (16 July 2020)**

86. The possibility that the personal data transferred between two economic operators for commercial purposes might undergo, at the time of the transfer or thereafter, processing for the purposes of public security, defence and State security by the authorities of that third country cannot remove that transfer from the scope of the GDPR.

87. […] it is patent from the very wording of Article 45(2)(a) of that regulation that no processing by a third country of personal data for the purposes of public security, defence and State security excludes the transfer at issue from the application of the regulation.

89. […] Article 2(1) and (2) of the GDPR must be interpreted as meaning that that regulation applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security. […]

91. As regards the level of protection required, it follows from a combined reading of those provisions that, in the absence of an adequacy decision under Article 45(3) of that regulation, a controller or processor may transfer personal data to a third country only if the controller or processor has provided 'appropriate safeguards', and on condition that 'enforceable data subject rights and effective legal remedies for data subjects' are available, such safeguards being able to be provided, inter alia, by the standard data protection clauses. […]

93. As the Advocate General stated in point 117 of his Opinion, the provisions of Chapter V of the GDPR are intended to ensure the continuity of that high level of protection where personal data is

transferred to a third country, in accordance with the objective set out in recital 6 thereof.

94. […] In that regard, although not requiring a third country to ensure a level of protection identical to that guaranteed in the EU legal order, the term 'adequate level of protection' must, as confirmed by recital 104 of that regulation, be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the regulation, read in the light of the Charter. […]

95. […] To that effect, recital 108 of the regulation states that, in the absence of an adequacy decision, the appropriate safeguards to be taken by the controller or processor in accordance with Article 46(1) of the regulation must 'compensate for the lack of data protection in a third country' in order to 'ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union'.

103. In that regard, although that provision does not list the various factors which must be taken into consideration for the purposes of assessing the adequacy of the level of protection to be observed in such a transfer, Article 46(1) of that regulation states that data subjects must be afforded appropriate safeguards, enforceable rights and effective legal remedies. […]

105. […] Article 46(1) and Article 46(2)(c) of the GDPR must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.

109. In addition, under Article 57(1)(f) of the GDPR, each supervisory authority is required on its territory to handle complaints which, in accordance with Article 77(1) of that regulation, any data subject is entitled to lodge where that data subject considers that the processing of his or her personal data infringes the regulation, and is required to examine the nature of that complaint as necessary. The supervisory authority must handle such a complaint with all due diligence […].

118. […], until such time as a Commission adequacy decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection (judgment of 6 October 2015, Schrems, C 362/14, EU:C:2015:650, paragraph 52 and the case-law cited) and, as a result, to suspend or prohibit transfers of personal data to that third country.

119. However, a Commission adequacy decision adopted pursuant to Article 45(3) of the GDPR cannot prevent persons whose personal data has been or could be transferred to a third country from lodging a complaint, within the meaning of Article 77(1) of the GDPR, with the competent national supervisory authority concerning the protection of their rights and freedoms in regard to the processing of that data. […]

121. […] Article 58(2)(f) and (j) of the GDPR must be interpreted as meaning that, unless there is a valid Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances

of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of the GDPR and by the Charter, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.

129. It should be noted in that regard that such a standard clauses decision differs from an adequacy decision adopted pursuant to Article 45(3) of the GDPR, which seeks, following an examination of the legislation of the third country concerned taking into account, inter alia, the relevant legislation on national security and public authorities' access to personal data, to find with binding effect that a third country, a territory or one or more specified sectors within that third country ensures an adequate level of protection and that the access of that third country's public authorities to such data does not therefore impede transfers of such personal data to the third country. Such an adequacy decision can therefore be adopted by the Commission only if it has found that the third country's relevant legislation in that field does in fact provide all the necessary guarantees from which it can be concluded that that legislation ensures an adequate level of protection.

132. In that regard, recital 109 of the regulation states that 'the possibility for the controller […] to use standard data-protection clauses adopted by the Commission […] should [not] prevent [it] […] from adding other clauses or additional safeguards' and states, in particular, that the controller 'should be encouraged to provide additional safeguards […] that supplement standard [data] protection clauses'.

134. […] It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses.

135. Where the controller or a processor established in the European Union is not able to take adequate additional measures to guarantee such protection, the controller or processor or, failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned. That is the case, in particular, where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data.

136. Therefore, the mere fact that standard data protection clauses in a Commission decision adopted pursuant to Article 46(2)(c) of the GDPR, such as those in the annex to the SCC Decision, do not bind the authorities of third countries to which personal data may be transferred cannot affect the validity of that decision. […]

142. It follows that a controller established in the European Union and the recipient of personal data are required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned. The recipient is, where appropriate, under an obligation, under Clause 5(b), to inform the controller of any inability to comply with those clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract.

143. If the recipient of personal data to a third country has notified the controller, pursuant to Clause 5(b) in the annex to the SCC Decision, that the legislation of the third country concerned does not allow him or her to comply with the standard data protection clauses in that annex, it follows from Clause 12 in that annex that data that has already been transferred to that third country and the copies thereof must be returned or destroyed in their entirety. In any event, under Clause 6 in that annex, breach of those standard clauses will result in a right for the person concerned to receive compensation for the damage suffered.

144. It should be added that, under Clause 4(f) in the annex to the SCC Decision, a controller established in the European Union undertakes, where special categories of data could be transferred to a third country not providing adequate protection, to inform the data subject before, or as soon as possible after, the transfer. That notice enables the data subject to be in a position to bring legal action against the controller pursuant to Clause 3(1) in that annex so that the controller suspends the proposed transfer, terminates the contract concluded with the recipient of the personal data or, where appropriate, requires the recipient to return or destroy the data transferred.

Furthermore, in order to avoid divergent decisions, Article 64(2) of the GDPR provides for the possibility for a supervisory authority which considers that transfers of data to a third country must, in general, be prohibited, to refer the matter to the European Data Protection Board (EDPB) for an opinion, which may, under Article 65(1)(c) of the GDPR, adopt a binding decision, in particular where a supervisory authority does not follow the opinion issued.

148. It follows that the SCC Decision provides for effective mechanisms which, in practice, ensure that the transfer to a third country of personal data pursuant to the standard data protection clauses in the annex to that decision is suspended or prohibited where the recipient of the transfer does not comply with those clauses or is unable to comply with them.

149. In the light of all of the foregoing considerations, the answer to the 7th and 11th questions is that examination of the SCC Decision in the light of Articles 7, 8 and 47 of the Charter has disclosed nothing to affect the validity of that decision.

156. […] the Privacy Shield Decision is binding on the supervisory authorities in so far as it finds that the United States ensures an adequate level of protection and, therefore, has the effect of authorising personal data transferred under the EU-US Privacy Shield. Therefore, until the Court should declare that decision invalid, the competent supervisory authority cannot suspend or prohibit a transfer of personal data to an organisation that abides by that privacy shield on the ground that it considers, contrary to the finding made by the Commission in that decision, that the US legislation governing the access to personal data transferred under that privacy shield and the use of that data by the public authorities of that third country for national security, law enforcement and other public interest purposes does not ensure an adequate level of protection.

157. The fact remains that, in accordance with the case-law set out in paragraphs 119 and 120 above, when a person lodges a complaint with the competent supervisory authority, that authority must examine, with complete independence, whether the transfer of personal data at issue complies with the requirements laid down by the GDPR and, if, in its view, the arguments put forward by that person with a view to challenging the validity of an adequacy decision are well founded, bring an action before the national courts in order for them to make a reference to the Court for a preliminary ruling for the purpose of examining the validity of that decision. […]

162. In order for the Commission to adopt an adequacy decision pursuant to Article 45(3) of the GDPR, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order (see, by analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015, Schrems, C 362/14, EU:C:2015:650, paragraph 96). […]

165. In the light of its general nature, the derogation set out in paragraph I.5 of Annex II to the Privacy Shield Decision thus enables interference, based on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States (see, by analogy, as regards Decision 2000/520, judgment of 6 October 2015, Schrems, C 362/14, EU:C:2015:650, paragraph 87). More particularly, as noted in the Privacy Shield Decision, such interference can arise from access to, and use of, personal data transferred from the European

Union to the United States by US public authorities through the PRISM and UPSTREAM surveillance programmes under Section 702 of the FISA and E.O. 12333.

173. […] it should also be observed that, under Article 8(2) of the Charter, personal data must, inter alia, be processed 'for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.

176. Lastly, in order to satisfy the requirement of proportionality according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing (see, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 140 and 141 and the case-law cited). […]

186. […] the first paragraph of Article 47 requires everyone whose rights and freedoms guaranteed by the law of the Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. According to the second paragraph of that article, everyone is entitled to a hearing by an independent and impartial tribunal.

188. To that effect, Article 45(2)(a) of the GDPR requires the Commission, in its assessment of the adequacy of the level of protection in a third country, to take account, in particular, of 'effective administrative and judicial redress for the data subjects whose personal data are being transferred'. Recital 104 of the GDPR states, in that regard, that the third country 'should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities', and adds that 'the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress'.

192. Furthermore, as regards both the surveillance programmes based on Section 702 of the FISA and those based on E.O. 12333, it has been noted in paragraphs 181 and 182 above that neither PPD 28 nor E.O. 12333 grants data subjects rights actionable in the courts against the US authorities, from which it follows that data subjects have no right to an effective remedy.

193. The Commission found, however, in recitals 115 and 116 of the Privacy Shield Decision, that, as a result of the Ombudsperson Mechanism introduced by the US authorities, as described in a letter from the US Secretary of State to the European Commissioner for Justice, Consumers and Gender Equality from 7 July 2016, set out in Annex III to that decision, and of the nature of that Ombudsperson's role, in the present instance, a 'Senior Coordinator for International Information Technology Diplomacy', the United States can be deemed to ensure a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter.

194. An examination […] must […] start from the premise that data subjects must have the possibility of bringing legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data.

196. […] there is nothing in that decision [Privacy Shield Decision] to indicate that that ombudsperson has the power to adopt decisions that are binding on those intelligence services and does not mention any legal safeguards that would accompany that political commitment on which data subjects could rely.

197. Therefore, the ombudsperson mechanism to which the Privacy Shield Decision refers does not

provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter.

199. It follows that Article 1 of the Privacy Shield Decision is incompatible with Article 45(1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter, and is therefore invalid.

200. Since Article 1 of the Privacy Shield Decision is inseparable from Articles 2 and 6 of, and the annexes to, that decision, its invalidity affects the validity of the decision in its entirety.

201. In the light of all of the foregoing considerations, it is to be concluded that the Privacy Shield Decision is invalid.

Maximillian Schrems v Data Protection Commissioner **(C-362/14), Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2015)**

46. Recital 60 in the preamble to Directive 95/46 states that transfers of personal data to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to the directive. In that regard, Chapter IV of the directive, in which Articles 25 and 26 appear, has set up a regime intended to ensure that the Member States oversee transfers of personal data to third countries. That regime is complementary to the general regime set up by Chapter II of the directive laying down the general rules on the lawfulness of the processing of personal data […]

63. Having regard to those considerations, where a person whose personal data has been or could be transferred to a third country which has been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46 lodges with a national supervisory authority a claim concerning the protection of his rights and freedoms in regard to the processing of that data and contests, in bringing the claim, as in the main proceedings, the compatibility of that decision with the protection of the privacy and of the fundamental rights and freedoms of individuals, it is incumbent upon the national supervisory authority to examine the claim with all due diligence. [...]

70. It is true that neither Article 25(2) of Directive 95/46 nor any other provision of the directive contains a definition of the concept of an adequate level of protection. In particular, Article 25(2) does no more than state that the adequacy of the level of protection afforded by a third country 'shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations' and lists, on a non-exhaustive basis, the circumstances to which consideration must be given when carrying out such an assessment.

71. However, first, as is apparent from the very wording of Article 25(6) of Directive 95/46, that provision requires that a third country 'ensures' an adequate level of protection by reason of its domestic law or its international commitments. Secondly, according to the same provision, the adequacy of the protection ensured by the third country is assessed 'for the protection of the private lives and basic freedoms and rights of individuals'. […]

73. The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph of the present Judgment would be disregarded. Furthermore, the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries. […]

75. Accordingly, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules, since it must, under Article 25(2) of Directive 95/46, take account of all the circumstances surrounding a transfer of personal data to a third country.

76. Also, in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted a decision pursuant to Article 25(6) of Directive 95/46, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard. […]

84. Under the fourth paragraph of Annex I to Decision 2000/520, the applicability of the safe harbour principles may be limited, in particular, 'to the extent necessary to meet national security, public interest, or law enforcement requirements' and 'by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non- compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation'[…]

87. In the light of the general nature of the derogation set out in the fourth paragraph of Annex I to Decision 2000/520, that decision thus enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States. To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference. […]

90. The Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.

91. As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data.

VII. COMMUNICATIONS DATA (METADATA)

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

Noting that, while metadata may provide benefits, certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of

communications and can give an insight into an individual's behaviour, social relationships, private preferences and identity,

**See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014)*

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

Acknowledging that, while metadata may provide benefits, certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications and can give an insight into an individual's behaviour, including their movements, social relationships, political activities, private preferences and identity,

**See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021); and UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019)*

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014)

[…] Shortly put, it is incompatible with existing concepts of privacy for States to collect all communications or metadata all the time indiscriminately. The very essence of the right to the privacy of communication is that infringements must be exceptional, and justified on a case-by-case basis. […]

***Big Brother Watch and Others v The United Kingdom*, Apps Nos 58170/13, 62322/14 and 24960/15, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

341. In both *Weber and Saravia* and *Liberty and Others* (cited above) the Court applied the above-mentioned six minimum safeguards developed in its case-law on targeted interception (see paragraph 335 above). However, while the bulk interception regimes considered in those cases were on their face similar to that in issue in the present case, both cases are now more than ten years old, and in the intervening years technological developments have significantly changed the way in which people communicate. Lives are increasingly lived online, generating both a significantly larger volume of electronic communications, and communications of a significantly different nature and quality, to those likely to have been generated a decade ago (see paragraph 322 above). The scope of the surveillance activity considered in those cases would therefore have been much narrower.

342. This is equally so with related communications data. As the ISR observed in its report, greater volumes of communications data are currently available on an individual relative to content, since every piece of content is surrounded by multiple pieces of communications data (see paragraph 159 above). While the content might be encrypted and, in any event, may not reveal anything of note about the sender or recipient, the related communications data could reveal a great deal of personal information, such as the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. Furthermore, any intrusion occasioned by the acquisition of related communications data will be magnified when they are obtained in bulk, since they are now capable of being analysed and interrogated so as to paint an intimate picture of a person through the mapping of social networks,

location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with (see paragraph 317 above).

363. For the reasons identified at paragraph 342 above, the Court is not persuaded that the acquisition of related communications data through bulk interception is necessarily less intrusive than the acquisition of content. It therefore considers that the interception, retention and searching of related communications data should be analysed by reference to the same safeguards as those applicable to content.

***Tele2 Sverige AB v Post- Och telestyrelsen* (C-203/15); *Secretary of State for the Home Department v Tom Watson et. al.* (C-698/16), Joined Cases, Judgment, Grand Chamber, Court of Justice of the European Union (21 December 2016)**

99. That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, that data provides the means [...] of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.

100. The interference entailed by such legislation in the fundamental rights enshrined in Articles 7 and 8 of the Charter is very far-reaching and must be considered to be particularly serious. The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance.

101. Even if such legislation does not permit retention of the content of a communication and is not, therefore, such as to affect adversely the essence of those rights, the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter.

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

Acknowledging that, while metadata may provide benefits, certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications and can give an insight into an individual's behaviour, social relationships private preferences and identity,

** See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/34/7 (23 March 2017)*

Report of the Special Rapporteur on the Promotion and Protection of Human Rights while Counter-Terrorism, Human Rights Implications of the Development, Use, Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism, UN Doc A/HRC/52/39 (1 March 2023)

45. The impact of surveillance on multiple human rights is considerable. The Special Rapporteur highlights that the right to privacy functions as a gateway right protecting and enabling many other

rights and freedoms, and its protection is intimately related to the existence and advancement of a democratic society. She therefore sees the escalation in the use of secret surveillance and the collection of content information and metadata for purposes of countering terrorism, combined with the runaway development of underregulated new technologies, as a significant threat to democratic societies.

Concluding Observations on the Third Periodic Report of Lebanon, Human Rights Committee, UN Doc CCPR/C/LBN/CO/3 (9 May 2018)

34. The State party should ensure that all laws governing surveillance activities, access to personal data and communications data (metadata) and any other interference with privacy are in full conformity with the Covenant, in particular article 17, including as regards the principles of legality, proportionality and necessity, and that State practice conforms thereto. It should, inter alia, ensure that (a) surveillance, collection of, access to and use of data and communications data are tailored to specific legitimate aims, are limited to a specific number of persons and are subject to judicial authorization; (b) effective and independent oversight mechanisms are in place to prevent arbitrary interference with privacy; and […] The State party should also ensure biometric data protection guarantees, in accordance with article 17 of the Covenant.

Concluding Observations on the Sixth Periodic Report of New Zealand, Human Rights Committee, UN Doc CCPR/C/NZL/CO/6 (28 April 2016)

16. The State party should take all appropriate measures to ensure that: ...(b) Sufficient judicial safeguards are implemented, regardless of the nationality or location of affected persons, in terms of interception of communications and metadata collection, processing and sharing.

***Shimovolos v Russia*, App No 30194/09, Judgment, European Court of Human Rights (21 June 2011)**

64. The Court reiterates that private life is a broad term not susceptible to exhaustive definition. Article 8 is not limited to the protection of an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. It also protects the right to establish and develop relationships with other human beings and the outside world. Private life may even include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".

65. The Court has earlier found that the systematic collection and storing of data by security services on particular individuals constituted an interference with these persons' private lives, even if that data was collected in a public place or concerned exclusively the person's professional or public activities. Collection, through a GPS device attached to a person's car, and storage of data concerning that person's whereabouts and movements in the public sphere was also found to constitute an interference with private life.

66. Turning to the circumstances of the present case, the Court observes that the applicant's name was registered in the Surveillance Database which collected information about his movements, by train or air, within Russia. Having regard to its case-law cited in paragraphs 64 and 65 above, the Court finds that the collection and storing of that data amounted to an interference with his private life as protected by Article 8 § 1 of the Convention.

***Uzun v Germany*, App No 35623/05, Judgment, European Court of Human Rights (2 September 2010)**

44. There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are

occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person walking along the street will inevitably be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain.

45. Further elements which the Court has taken into account in this respect include the question whether there has been compilation of data on a particular individual, whether there has been processing or use of personal data or whether there has been publication of the material concerned in a manner or degree beyond that normally foreseeable.

46. Thus, the Court has considered that the systematic collection and storing of data by security services on particular individuals, even without the use of covert surveillance methods, constituted an interference with these persons' private lives. [...]

47. The Court has further taken into consideration whether the impugned measure amounted to a processing or use of personal data of a nature to constitute an interference with respect for private life. Thus, it considered, for instance, the permanent recording of footage deliberately taken of the applicant at a police station by a security camera and its use in a video identification procedure as the processing of personal data about the applicant interfering with his right to respect for private life. Likewise, the covert and permanent recording of the applicants' voices at a police station for further analysis as voice samples directly relevant for identifying these persons in the context of other personal data was regarded as the processing of personal data about them amounting to an interference with their private lives. [...]

51. By the surveillance of the applicant via GPS, the investigation authorities, for some three months, systematically collected and stored data determining, in the circumstances, the applicant's whereabouts and movements in the public sphere. They further recorded the personal data and used it in order to draw up a pattern of the applicant's movements, to make further investigations and to collect additional evidence at the places the applicant had travelled to, which was later used at the criminal trial against the applicant.

52. In the Court's view, GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings. Having regard to the principles established in its case-law, it nevertheless finds the above-mentioned factors sufficient to conclude that the applicant's observation via GPS, in the circumstances, and the processing and use of the data obtained thereby in the manner described above amounted to an interference with his private life as protected by Article 8 § 1. [...]

66. While the Court is not barred from gaining inspiration from [the Weber principles], it finds that these rather strict standards, set up and applied in the specific context of surveillance of telecommunications, are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations. It will therefore apply the more general principles on adequate protection against arbitrary interference with Article 8 rights as summarised above. [...]

69. In examining whether domestic law contained adequate and effective guarantees against abuse, the Court observes that in its nature conducting surveillance of a person by building a GPS receiver into the car he or she uses, coupled with visual surveillance of that person, permits the authorities to track that person's movements in public places whenever he or she is travelling in that car. It is true that, as the applicant had objected, there was no fixed statutory limit on the duration of such

monitoring. A fixed time-limit had only subsequently been enacted in so far as under the new Article163f § 4 of the Code of Criminal Procedure, the systematic surveillance of a suspect ordered by a Public Prosecutor could not exceed one month, and any further extension could only be ordered by a judge. However, the Court is satisfied that the duration of such a surveillance measure was subject to its proportionality in the circumstances and that the domestic courts reviewed the respect of the proportionality principle in this respect. It finds that German law therefore provided sufficient guarantees against abuse on that account.

***Draft Agreement between Canada and the European Union on the Transfer of Passenger Name Record Data* (1/15), Court of Justice of the European Union, Grand Chamber, Opinion pursuant to Article 218(11) TFEU (26 July 2017)**

121. As set out in the Annex to the envisaged agreement, the PNR data covered by that agreement includes, inter alia, and besides the name(s) of the air passenger(s), information necessary to the reservation, such as the dates of intended travel and the travel itinerary, information relating to tickets, groups of persons checked-in under the same reservation number, passenger contact information, information relating to the means of payment or billing, information concerning baggage and general remarks regarding the passengers […]

122. Since the PNR data therefore includes information on identified individuals, namely air passengers flying between the European Union and Canada, the various forms of processing to which, under the envisaged agreement, that data may be subject, namely its transfer from the European Union to Canada, access to that data with a view to its use or indeed its retention, affect the fundamental right to respect for private life […]

***Digital Rights Ireland Ltd v Minister of Communications, Marine and Natural Resources et al.* (C-293/12)*; Kärntner Landesregierung and others* (C-594/12), Joined Cases, Judgment, Grand Chamber, Court of Justice of the European Union (8 April 2014)**

26. […] it should be observed that the data which providers of publicly available electronic communications services or of public communications networks must retain, pursuant to Articles 3 and 5 of Directive 2006/24, include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

27. Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.

28. In such circumstances, even though, as is apparent from Article 1(2) and Article 5(2) of Directive 2006/24, the directive does not permit the retention of the content of the communication or of information consulted using an electronic communications network, it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users,

of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter.

29. The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article.

VIII. ACCESS TO REMEDY: VICTIMHOOD, STANDING, AND NOTIFICATION

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

7. *Calls upon* all States: (f) To provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations [...]

**See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014)*

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

10. Calls upon all States: (h) To develop or maintain and implement adequate legislation, with effective sanctions and remedies, that protects individuals against violations and abuses of the right to privacy, namely through the collection, processing, retention or use of personal data by individuals, Governments, business enterprises or private organizations without the individual's free, explicit and informed consent or unless otherwise unlawful, in accordance with international human rights law;

** See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019)*

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

56. […] OHCHR recommends that States: (h) Ensure that victims of human rights violations and abuses linked to the use of surveillance systems have access to effective remedies.

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

50. Victims of privacy violations or abuses committed by States and/or business enterprises must have access to an effective remedy. States not only have obligations to ensure accountability and remedy for human rights violations committed by State actors, they must also take appropriate steps to ensure that victims of business-related human rights abuse have access to an effective

remedy (see pillar III of the Guiding Principles on Business and Human Rights). Depending on the nature of a particular case or situation, victims should be able to achieve remedies through effective judicial or non-judicial State-based grievance mechanisms (A/HRC/32/19, Corr. 1 and Add. 1 and A/HRC/38/20 and Add. 1). Relevant State-based non-judicial mechanisms in the ICT context include independent authorities with powers to monitor State and private sector data privacy practices, such as privacy and data protection bodies.

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

40. Effective remedies for violations of privacy through digital surveillance can thus come in a variety of judicial, legislative or administrative forms. Effective remedies typically share certain characteristics. First, those remedies must be known and accessible to anyone with an arguable claim that their rights have been violated. Notice (that either a general surveillance regime or specific surveillance measures are in place) and standing (to challenge such measures) thus become critical issues in determining access to effective remedy. States take different approaches to notification: while some require post facto notification of surveillance targets, once investigations have concluded, many regimes do not provide for notification. Some may also formally require such notification in criminal cases; however, in practice, this stricture appears to be regularly ignored. There are also variable approaches at national level to the issue of an individual's standing to bring a judicial challenge. The European Court of Human Rights ruled that, while the existence of a surveillance regime might interfere with privacy, a claim that this created a rights violation was justiciable only where there was a "reasonable likelihood" that a person had actually been subjected to unlawful surveillance.

41. Second, effective remedies will involve prompt, thorough and impartial investigation of alleged violations. This may be provided through the provision of an "independent oversight body [...] governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society." Third, for remedies to be effective, they must be capable of ending ongoing violations, for example, through ordering deletion of data or other reparation. Such remedial bodies must have "full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders". Fourth, where human rights violations rise to the level of gross violations, non-judicial remedies will not be adequate, as criminal prosecution will be required.

46. A central part of human rights due diligence as defined by the Guiding Principles is meaningful consultation with affected stakeholders. In the context of information and communications technology companies, this also includes ensuring that users have meaningful transparency about how their data are being gathered, stored, used and potentially shared with others, so that they are able to raise concerns and make informed decisions. The Guiding Principles clarify that, where enterprises identify that they have caused or contributed to an adverse human rights impact, they have a responsibility to ensure remediation by providing remedy directly or cooperating with legitimate remedy processes. To enable remediation at the earliest possible stage, enterprises should establish operational-level grievance mechanisms.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

21. Targets of surveillance suffer interference with their rights to privacy and freedom of opinion and expression whether the effort to monitor is successful or not. The target need have no knowledge of the attempted or successful intrusion for the interference with their right to privacy to be complete […].

28. It is clear from the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework adopted by the Human Rights Council in 2011, that a State's duty to protect includes a duty to take appropriate steps to prevent, investigate, punish and redress human rights abuse by third parties (A/HRC/17/31). In the Guiding Principles, States are urged to exercise adequate oversight in order to meet their international human rights obligations when they contract with, or legislate for, business enterprises to provide services that may have an impact on the enjoyment of human rights (ibid., p. 10).

39. […] The Human Rights Committee has stressed that law enforcement and prosecutorial authorities should investigate allegations of violations promptly, thoroughly and effectively through independent and impartial bodies. The duty to provide effective remedies also entails an obligation to protect individuals from acts by private sector entities that cause infringements, by exercising due diligence to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities.

40. Victims of targeted surveillance have had little success in their efforts to obtain recognition of the harm suffered, let alone remedies for such harm. […]

41. Litigation as a course of action to seek remedy against private surveillance companies that manufacture and sell tools and Governments that deploy them is uncertain. […] The lack of causes of action and remedies raises serious concerns about the likelihood of holding companies accountable for human rights violations. Alleged victims have commenced litigation or formal complaints against private surveillance companies or Governments in at least eight countries. However, the barriers to successful litigation and formal complaints are significant, including the lack of judicial oversight, remedies, causes of action, enforcement and data preservation.

42. In some cases, civil society organizations have requested that Governments investigate unlawful surveillance, but these requests are frequently rejected. […] Even when States open investigations to determine whether government surveillance violated human rights norms or State laws, the investigations can be arbitrary or disorganized.

54. […] Some claims may be difficult to pursue because of the difficulty and expense of proving the existence of surveillance or attributing the surveillance to State actors – or even to specific State agencies that would be the targets of a lawsuit. Individual targets of surveillance often do not know of the surveillance being carried out against them – or, if they do, it may be beyond the tolling of a statute of limitations. It is, in other words, extremely rare for a claimant to succeed in domestic legal claims arising from allegedly unlawful surveillance.

55. […] National legislation should also establish causes of action against private entities that take into account changes in corporate ownership (known as "disposals" or "makeovers"), which often complicate the efforts of victims to seek accountability and redress.

56. At the same time, targeted surveillance is not always territorially contained. When States reach beyond their borders to conduct targeted surveillance, it may be difficult for the individuals targeted by such surveillance to bring claims against the offending State. Some of the same evidentiary and other burdens as in domestic claims may be present in these cases as well. Moreover, as in the *Doe* case noted above, courts may be unwilling to entertain lawsuits against foreign sovereigns. While the rules for such suits vary, States should interpret the norms of sovereign immunity to ensure that their courts may entertain suits against foreign Governments.

66. For States: (b) States that purchase or use surveillance technologies ("purchasing States") should ensure that domestic laws permit their use only in accordance with the human rights standards of legality, necessity and legitimacy of objectives, and establish legal mechanisms of redress consistent with their obligation to provide victims of surveillance-related abuses with an

effective remedy.

Report of the Special Rapporteur on the Situation of Human Rights Defenders, Situation of Women Human Rights Defenders, UN Doc A/HRC/40/60 (10 January 2019)

8. It is not possible to fully exercise the right to defend and promote human rights without also protecting the right to access to justice when violations occur that restrict that right. In other words, the protection of human rights defenders involves not only strengthening security measures in their favour, but also mitigating risks, addressing threats and obstacles and exercising due diligence in investigations of violence against them and other violations of their rights.

Concluding Observations on Equatorial Guinea in the Absence of Its Initial Report, Human Rights Committee, UN Doc CCPR/C/GNQ/CO/1 (22 August 2019)

51. The State party should ensure: (c) that affected persons have proper access to effective remedies in cases of abuse.

Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, UN Doc CCPR/C/ITA/CO/6 (28 March 2017)

37. The State party should review the regime regulating the interception of personal communications, hacking of digital devices and the retention of communications data with a view to ensuring: (b) that robust independent oversight systems over surveillance, interception and hacking, including by providing for judicial involvement in the authorization of such measures in all cases and affording persons affected with effective remedies in cases of abuse, including, where possible, an ex post notification that they were subject to measures of surveillance or hacking."

***Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, App No 62540/00, Judgment, European Court of Human Rights (28 June 2007)**

58. […] In all these cases the Court found that to the extent that a law institutes a system of surveillance under which all persons in the country concerned can potentially have their mail and telecommunications monitored, without their ever knowing this unless there has been either some indiscretion or subsequent notification, it directly affects all users or potential users of the postal and telecommunication services in that country. The Court therefore accepted that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting them, without having to allege that such measures were in fact applied to him or her.

In line with its holdings in these cases, the Court finds that the second applicant, being an individual, can claim to be victim, within the meaning of Article 34, on account of the very existence of legislation in Bulgaria permitting secret surveillance. It notes in this connection that the applicants do not contend that measures of surveillance were actually applied to them; it is therefore inappropriate to apply a reasonable-likelihood test to determine whether they may claim to be victims of a violation of their Article 8 rights.

60. As regards the applicant association, the Court notes that it has already held that a legal person is entitled to respect for its "home" within the meaning of Article 8 § 1 of the Convention. The applicant association is therefore, contrary to what the Government suggest, not wholly deprived of the protection of Article 8 by the mere fact that it is a legal person. While it may be open to doubt whether, being such a person, it can have a "private life" within the meaning of that provision, it can be said that its mail and other communications, which are in issue in the present case, are covered by the notion of "correspondence" which applies equally to communications

originating from private and business premises. The former Commission has already held, in circumstances identical to those of the present case, that applicants who are legal persons may fear that they are subjected to secret surveillance. It has accordingly accepted that they may claim to be victims. […]

90. Finally, the Court notes that under Bulgarian law the persons subjected to secret surveillance are not notified of this fact at any point in time and under any circumstances. According to the Court's case-law, the fact that persons concerned by such measures are not apprised of them while the surveillance is in progress or even after it has ceased cannot by itself warrant the conclusion that the interference was not justified under the terms of paragraph 2 of Article 8, as it is the very unawareness of the surveillance which ensures its efficacy. However, as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned. Indeed, the German legislation in issue in the cases of *Klass and Others* and *Weber and Saravia*, as modified by the German Federal Constitutional Court, did provide for such notification. The position in the *Leander* case was similar.

91. By contrast, the SSMA does not provide for notification of persons subjected to surreptitious monitoring under any circumstances and at any point in time. On the contrary, section 33 of the SSMA, as construed by the Supreme Administrative Court, expressly prohibits the disclosure of information whether a person has been subjected to surveillance, or even whether warrants have been issued for this purpose. Indeed, such information is considered classified. The result of this is that unless they are subsequently prosecuted on the basis of the material gathered through covert surveillance, or unless there has been a leak of information, the persons concerned cannot learn whether they have ever been monitored and are accordingly unable to seek redress for unlawful interferences with their Article 8 rights. Bulgarian law thus eschews an important safeguard against the improper use of special means of surveillance.

UN General Assembly Resolution on the Promotion and Protection of Human Right in the Context of Digital Technologies, UN Doc A/RES/78/213 (19 December 2023)

16. *Calls upon* Member States to ensure that […] that legal mechanisms of redress and effective remedies are available for victims of surveillance-related violations and abuses;

UN General Assembly Resolution on Terrorism and Human Rights, UN Doc A/RES/78/210 (19 December 2023)

30. *Urges* States to safeguard the right to privacy in accordance with international law, in particular international human rights law, and to take measures to ensure that interference with or restriction of that right are not arbitrary, are adequately regulated by law and are subject to effective oversight and appropriate redress, including through judicial review or other means;

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

7. Calls upon all States: (f) To provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations;

** See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on*

the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014)

UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/51/9 (6 October 2022)*

11. *Calls upon* States: (m) To ensure that targeted surveillance technologies are only used in accordance with the human rights principles of lawfulness, legitimacy, necessity and proportionality, and that legal mechanisms of redress and effective remedies are available for victims of surveillance-related violations and abuses;

**See also UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/45/18 (12 October 2020)*

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

25. [The Human Rights Committee] determined that the right to privacy required that robust, independent oversight systems were in place regarding surveillance, interception and hacking, including by ensuring that the judiciary was involved in the authorization of such measures, in all cases, and by affording persons affected with effective remedies in cases of abuse, including, where possible, an ex post notification that they had been placed under surveillance or that their data had been hacked (ibid., para. 37).

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014)

61. […] In addition, individuals should have the right to seek an effective remedy for any alleged violation of their online privacy rights. This requires a means by which affected individuals can submit a complaint to an independent mechanism that is capable of conducting a thorough and impartial review, with access to all relevant material and attended by adequate due process guarantees. Accountability mechanisms can take a variety of forms, but must have the power to order a binding remedy. […] States should not impose standing requirements that undermine the right to an effective remedy.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/23/40 (17 April 2013)

82. Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/HRC/13/37 (28 December 2009)

53. […] The Special Rapporteur therefore calls for increased internal oversight to complement the processes for independent authorization and external oversight. This internal and external accountability system will ensure that there are effective remedies for individuals, with meaningful access to redress mechanisms.

Concluding Observations on the Second Periodic Report of Indonesia, Human Rights Committee, UN Doc CCPR/C/IDN/CO/2, (26 March 2024)

37. […], the State party should: (c) Ensure that all allegations of harassment, intimidation, surveillance and excessive use of force are investigated promptly, thoroughly and impartially, that those found responsible are prosecuted and, if found guilty, punished and that victims are afforded effective remedies;

Concluding Observations on the Fifth Periodic Report of the Republic of Korea, Human Rights Committee, UN Doc CCPR/C/KOR/CO/5 (30 October 2023)

50. The State party should: (c) Ensure that affected persons are notified of the surveillance and interception activities to which they have been subjected, where possible, and that they have access to effective remedies in cases of abuse.

Concluding Observations on the Fifth Periodic Report of the United States of America, Human Rights Committee, UN Doc CCPR/C/USA/CO/5 (30 October 2023)

57. […]. It should ensure that those responsible are brought to justice and, if found guilty, punished with appropriate sanctions, and that victims of human rights violations and abuses linked to the use of surveillance systems have access to effective remedies.

Concluding Observations on the Fourth Periodic Report of the Islamic Republic of Iran, Human Rights Committee, UN Doc CCPR/C/IRN/CO/4 (26 October 2023)

46. […] The State party should […] ensure access to effective remedies.

Concluding Observations on the Eighth Periodic Report of Colombia, UN Doc CCPR/C/COL/CO/8 (21 July 2023)

31. […] The State party should also ensure […] that there is access to effective remedies in cases of abuse.

Concluding Observations on the Initial Report of the State of Palestine, UN Doc CCPR/C/PSE/CO/1 (21 July 2023)

38. In the light of the Committee's general comment No. 16 (1988) on right to privacy, the State party should: (d) Strengthen existing monitoring mechanisms to ensure that all allegations of abuse are thoroughly investigated, that such investigations lead to appropriate sanctions where warranted and that victims have access to effective remedies in cases of abuse.

Concluding Observations on the Fourth Periodic Report of Zambia, Human Rights Committee, UN Doc CCPR/C/ZMB/CO/4 (20 March 2023)

32. […] The State party should also […] ensure access to effective remedies in cases of abuse.

Concluding Observations on the Third Periodic Report of Turkmenistan, UN Doc CCPR/C/TKM/CO/3 (17 March 2023)

38. The Committee reiterates its concern about the lack of a clear legal framework regulating surveillance activities, including by the intelligence services. It regrets the absence of the effective investigation of allegations of human rights violations, including in relation to surveillance by law enforcement officials, and the failure of the State party to provide redress to victims (art. 17).

39. […] the Committee urges the State party to: (c) Conduct effective investigations into all allegations of human rights violations, including those resulting from surveillance by law enforcement agencies, and provide appropriate redress to victims.

Concluding Observations on the Seventh Periodic Report of Japan, Human Rights Committee, UN Doc CCPR/C/JPN/CO/7 (28 October 2022)

35. [The State Party] should ensure that any interference with the right to privacy requires prior authorization by a court and is subject to effective and independent oversight mechanisms, and that affected persons are notified of the surveillance and interception activities to which they are being subjected, where possible, and have access to effective remedies in cases of abuse. The State party should also ensure that all reports of abuse are thoroughly investigated and that such investigations lead to appropriate sanctions where warranted.

Concluding Observations on the Fifth Periodic Report of the Philippines, Human Rights Committee, UN Doc CCPR/C/PHL/CO/5 (28 October 2022)

14. The State party should: (d) Ensure that any interference with the right to privacy, including through the publication of the personal data of individuals suspected of terrorist acts and surveillance activities, requires […] that affected persons are, where possible, notified of the surveillance and interception activities to which they are being subjected and have access to effective remedies in cases of abuse;

Concluding Observations on the Fourth Periodic Report of Hong Kong, China, Human Rights Committee, UN Doc CCPR/C/CHN-HKG/CO/4 (22 July 2022)

40. Hong Kong, China, should: (c) […] ensure access to effective remedies in cases of abuse;

Concluding Observations on the Fifth Periodic Report of Ireland, Human Rights Committee, UN Doc CCPR/C/IRL/CO/5 (22 July 2022)

46. […] The State party should also ensure […] that there is access to effective remedies in cases of abuse.

Concluding Observations on the Seventh Periodic Report of Germany, Human Rights Committee, UN Doc CCPR/C/DEU/CO/7 (11 November 2021)

42. The Committee is concerned about the wide reaching powers of surveillance, including online surveillance and the hacking of encrypted communications data during criminal investigations. […]

43. […] The State party should also […] ensure access to effective remedies in cases of abuse.

Concluding Observations on the Sixth Periodic Report of Belgium, Human Rights Committee, UN Doc CCPR/C/BEL/CO/6 (6 December 2019)

11. […] It also remains concerned about the absence of legal guarantees relating to the collection and processing of data on persons in various databases related to efforts to prevent and combat terrorism and violent extremism […].

12. The State party should: (b) Provide legal guarantees for individuals whose nationalities, residence permits or passports have been revoked and/or who are included in the various databases related to efforts to prevent and combat terrorism and violent extremism, including effective remedies; […]

Concluding Observations on the Third Periodic Report of Tajikistan, Human Rights

Committee, UN Doc CCPR/C/TJK/CO/3 (22 August 2019)*

42. The State party should ensure that: (…) (c) the persons affected have proper access to effective remedies in cases of abuse.

**See also Concluding Observations on the Fifth Periodic Report of Belarus, Human Rights Committee, UN Doc CCPR/C/BLR/CO/5 (22 November 2018), para 44; Concluding Observations on the Third Periodic Report of Lebanon, Human Rights Committee, UN Doc CCPR/C/LBN/CO/3 (9 May 2018), para 34; Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/7 (17 August 2015), para 24*

Concluding Observations on the Fourth Periodic Report of Estonia, Human Rights Committee, UN Doc CCPR/C/EST/CO/4 (18 April 2019)

30. The State party should bring its regulations governing data retention and access thereto, surveillance and interception activities, and those relating to the intelligence-sharing of personal communications, into full conformity with the Covenant, in particular article 17, including with the principles of legality, proportionality and necessity. It should ensure that […] (c) persons affected are notified of surveillance and interception activities, where possible, and have access to effective remedies in cases of abuse.

Concluding Observations on the Fourth Periodic Report of Bulgaria, Human Rights Committee, UN Doc CCPR/C/BGR/CO/4 (15 November 2018)

34. The State party should review its legislation in order to bring it into line with its obligations under the Covenant. It should, in particular: […] (c) Ensure that surveillance activities conform with its obligations under article 17 of the Covenant, including […] that persons affected by these measures have access to effective remedies;

Concluding Observations on the Sixth Periodic Report of Hungary, Human Rights Committee, UN Doc CCPR/C/HUN/CO/6 (9 May 2018)

43. […] It is also concerned at the lack of provision for effective remedies in cases of abuse and the absence of a requirement to notify the person under surveillance as soon as possible, without endangering the purpose of the restriction, after the termination of the surveillance measure (arts. 2, 17, 19 and 26).

Concluding Observations on the Second Periodic Report of Honduras, Human Rights Committee, UN Doc CCPR/C/HND/CO/2 (27 July 2017) (translated from the original Spanish)

38. The Committee is concerned about allegations regarding the frequent application of the Special Law on the Interception of Private Communications, which entails extensive monitoring of private communications. It also concerned about [...] the lack of adequate monitoring mechanisms to continuously review the application of the Special Law; And the difficulty of obtaining judicial redress from victims of unlawful surveillance.

39. The State party should [...] ensure that the implementation of the Special Law on the Interception of Private Communications is subject to continuous and adequate monitoring by means of an independent monitoring mechanism which provides victims with adequate remedies."

Concluding Observations on the Second Periodic Report of Turkmenistan, Human Rights Committee, UN Doc CCPR/C/TKM/CO/2 (28 March 2017)

37. The State party should ensure that: (c) affected persons have proper access to effective remedies in cases of abuse.

Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee, UN Doc CCPR/C/POL/CO/7 (4 November 2016)

39. […] The Committee is particularly concerned about: f) the lack of notification, complaints procedure or mechanism for remedies.

Concluding Observations on the Third Periodic Report of the Former Yugoslav Republic of Macedonia, Human Rights Committee, UN Doc CCPR/C/MKD/CO/3 (17 August 2015)

23. [...] [The State Party should] ensure that persons who are unlawfully monitored are systematically informed thereof and have access to adequate remedies.

***Wieder and Guarnieri v the United Kingdom*, Apps Nos 64371/16 and 64407/16, Judgment, European Court of Human Rights (12 September 2023)**

97. In determining victim status the Court must first have regard to the scope of the legislation permitting secret surveillance measures by examining whether applicants could possibly be affected by it, either because they belong to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Where domestic law provides an effective remedy for persons who believe that their communications have been intercepted, such persons may claim to be victims of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if they are able to show that, due to their personal situation, they are potentially at risk of being subjected to such measures (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 171, ECHR 2015).

98. It follows that, in a case such as the present, where domestic law provided a remedy for all persons who believed that their communications had been intercepted (see paragraphs 28-30 above; see also *Big Brother Watch and Others*, cited above, 271), potential applicants may claim to be a victim of a violation occasioned by the mere existence of the section 8(4) regime only if they are able to substantiate their claim that they belonged to a group of people who could have been directly affected by the surveillance regime, and that, due to their personal situation, their electronic communications were potentially at risk of being intercepted, stored and searched by the United Kingdom intelligence agencies pursuant to the section 8(4) regime.

99. For the purposes of the Article 8 complaint the level of persuasion necessary to establish victim status cannot be unreasonably high. The section 8(4) regime is a bulk interception regime and communications may be intercepted, stored and searched even if neither the sender nor recipient is of interest to the intelligence agencies. Moreover, the nature of electronic communications is such that the sender will not know which countries his communications passed through *en route* to the recipients, and cannot, therefore, know which States' intelligence agencies might have had the opportunity to intercept them. Nonetheless, as the Convention does not provide for the institution of an *actio popularis* or for a review the relevant law and practice in *abstracto* (see *Roman Zakharov*, cited above, § 164), potential applicants must take steps to substantiate their claim that they were potentially at risk of having their communications intercepted, searched and possibly even examined under the impugned surveillance regime.

***Ekimdzhiev and Ors v Bulgaria*, App No 70078/12, Judgment, European Court of Human Rights (11 January 2022)**

348. The relevant factors under this rubric are (a) when is such notification possible, and (b) whether it is a prerequisite for using the available remedies.

349. As already noted in paragraph 267 above, the National Bureau must notify someone who has been placed under secret surveillance only if that has happened unlawfully, whereas under the Court's case-law such notification is, in the absence of a remedy available without prior notification, required in all cases, as soon as it can be made without jeopardising the purpose of the surveillance (see *Klass and Others v. Germany*, 6 September 1978, § 58, Series A no. 28; *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 135, ECHR 2006-XI; and, more recently, *Roman Zakharov*, cited above, § 287). […] Moreover, the Bureau is only required to notify individuals, not legal persons (see paragraph 130 above) […]

352. In 2009 Bulgaria put in place a dedicated remedy in respect of secret surveillance: a claim for damages under section 2(1)(7) of the 1988 Act (see paragraph 136 above). But that remedy, although effective in some scenarios, suffers from three serious limitations outlined in paragraphs 266 to 273 above: (a) it has so far not been able to operate in the absence of prior notification by the National Bureau that someone has been placed under surveillance, (b) it does not entail an examination of the necessity for the surveillance in each case, and (c) it is not open to legal persons.

353. Moreover, the only form of relief available in such proceedings is money damages (see paragraph 139 above); the courts have no power to order the destruction of surveillance material (contrast, for instance, *Big Brother Watch and Others*, cited above, 413). […]

355. It follows that Bulgarian law does not provide an effective remedy to all persons suspecting, without concrete proof, that they have been unjustifiably subjected to secret surveillance. It also follows that the Government's objection that domestic remedies have not been exhausted, which was joined to the merits (see paragraph 259 above), must be rejected.

379. Neither the 2007 Act nor Article 159a of the Code of Criminal Procedure provide for a remedy with respect to the retention or accessing of communications data.

380. Nothing suggests that the remedies under section 38(1) and (7), section 39(1) and (2), and section 82(1) of the 2002 Act, as worded after the 2019 amendment intended to transpose Directive (EU) 2016/680 (see paragraphs 218 and 227 above), have so far been used to provide redress with respect to the retention of communications data by communications service providers or with respect to its accessing and use by the authorities. […] In the absence of further particulars about the actual operation of those remedies with respect to communications data, it cannot be accepted that they are currently effective in that respect. Moreover, those remedies are not open to legal persons (see paragraphs 216 and 239 above).

381. Nor is there any evidence that a remedy is available under the general law of tort.

382. It follows that the public's misgivings about the threat of abusive accessing and use of communications data by the authorities cannot be sufficiently dispelled by the presence of effective remedies in that respect.

416. The 2007 Act requires the special parliamentary committee to notify an individual if his or her retained communications data has been accessed or sought to be accessed unlawfully, if such notification would not defeat the purpose for which those data has been accessed (see paragraph 213 above). However, as noted in paragraph 349 above in relation to secret surveillance, under the Court's case-law such notification is required in all cases, not only those in which the data has been accessed unlawfully, as soon as the notification can be made without jeopardising the purpose of the measure.

418. As already noted in paragraphs 379 to 381 above, it has not been shown that an effective remedy exists in Bulgaria in respect of the retention and accessing of communications data. The Government's objection that the applicants have not exhausted domestic remedies in that respect, which was joined to the merits (see paragraph 368 above), must therefore be rejected.
***Svetova and Others v Russia*, App No 54714/17, Judgment, European Court of Human Rights (24 January 2023)**

45. Lastly, the Court notes that the Russian courts declined to consider the applicants' complaint about the legality and the manner in which the search and seizure measures had been executed. They held that those matters would be examined at some future point in time during a criminal trial. This, however, had the practical effect of denying an effective review of the applicants' grievances in so far as they were not the individuals being investigated and had no status in any criminal proceedings. It follows that they were denied an effective remedy required by Article 13 of the Convention.

***Zoltán Varga v Slovakia*, App No 58361/12 and 2 others, Judgment, European Court of Human Rights (20 July 2021)**

108. In that connection, the Court reiterates that a decision or measure favourable to the applicant is not, in principle, sufficient to deprive him or her of the status of "victim" for the purposes of Article 34 of the Convention unless the national authorities have acknowledged, either expressly or in substance, and then afforded redress for, the breach of the Convention […].

109. As to the destruction of the primary material originating from the implementation of warrants 1 and 2 in the control of the SIS and the other material resulting from the implementation of all three warrants in the control of the Regional Court, the reason indicated was, respectively, that the material was unusable (see paragraph 14 above) and that its archiving period had expired (see paragraph 17 above). In other words, there was no acknowledgment, express or implied, of a violation of the applicant's rights, let alone any other redress with regard to the past existence of that material being afforded or at least arguably available.

110. […] Nevertheless, noting the scope of that finding and the reasons behind it, the Court considers that it fails to address the essence of the applicant's complaints, in so far as they have to do with the existence of adequate safeguards against abuse and other aspects of the lawfulness of the implementation of the three warrants in Convention terms.

***Big Brother Watch and Others v The United Kingdom*, Apps Nos 58170/13, 62322/14 and 24960/15, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

337. […] the question of subsequent notification of surveillance measures is a relevant factor in assessing the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of surveillance powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively [see *Roman Zakharov*, cited above, § 233; see also *Klass and Others v. Germany*, 6 September 1978, §§ 55 and 56, Series A no. 28] or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts, whose jurisdiction does not depend on notification to the surveillance subject of the measures taken (see *Roman Zakharov*, cited above, § 234; see also *Kennedy*, cited above, § 167).

357. Finally, an effective remedy should be available to anyone who suspects that his or her communications have been intercepted by the intelligence services, either to challenge the lawfulness of the suspected interception or the Convention compliance of the interception regime. In the targeted interception context, the Court has repeatedly found the subsequent notification of surveillance measures to be a relevant factor in assessing the effectiveness of remedies before the

courts and hence the existence of effective safeguards against the abuse of surveillance powers. However, it has acknowledged that notification is not necessary if the system of domestic remedies permits any person who suspects that his or her communications are being or have been intercepted to apply to the courts; in other words, where the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his or her communications (see *Roman Zakharov*, cited above, § 234 and *Kennedy*, cited above, § 167).

358. The Court considers that a remedy which does not depend on notification to the interception subject could also be an effective remedy in the context of bulk interception; in fact, depending on the circumstances it may even offer better guarantees of a proper procedure than a system based on notification. Regardless of whether material was acquired through targeted or bulk interception, the existence of a national security exception could deprive a notification requirement of any real practical effect. The likelihood of a notification requirement having little or no practical effect will be more acute in the bulk interception context, since such surveillance may be used for the purposes of foreign intelligence gathering and will, for the most part, target the communications of persons outside the State's territorial jurisdiction. Therefore, even if the identity of a target is known, the authorities may not be aware of his or her location.

359. The powers and procedural guarantees an authority possesses are relevant in determining whether a remedy is effective. Therefore, in the absence of a notification requirement it is imperative that the remedy should be before a body which, while not necessarily judicial, is independent of the executive and ensures the fairness of the proceedings, offering, in so far as possible, an adversarial process. The decisions of such authority shall be reasoned and legally binding with regard, *inter alia*, to the cessation of unlawful interception and the destruction of unlawfully obtained and/or stored intercept material (see, *mutatis mutandis*, *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 120, ECHR 2006-VII and also *Leander*, cited above, §§ 81-83 where the lack of power to render a legally binding decision constituted a main weakness in the control offered)."

***Centrum för Rättvisa v Sweden*, App No 35252/08, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

169. It must be seen, therefore, whether, as alleged by the applicant, the impugned legislation institutes a system of secret surveillance that potentially affects all persons communicating over the telephone or using the internet.

175. In the context of the issue of victim status, without prejudice to the conclusions to be drawn in respect of the substantive requirements of Article 8 § 2 and Article 13 in the present case, the Court notes that the domestic remedies available in Sweden to persons who suspect that they are affected by bulk interception measures are subject to a number of limitations. In the Court's view, even if these limitations are to be considered inevitable or justified, the practical result is that the availability of remedies cannot sufficiently dispel the public's fears related to the threat of secret surveillance.

176. It follows that it is not necessary to examine whether the applicant, due to its personal situation, is potentially at risk of seeing its communications or related data intercepted and analysed.

177. On the basis of the above considerations the Court finds that an examination of the relevant legislation *in abstracto* is justified. […]

251. […] There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively […] or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts, whose jurisdiction does not depend on notification to the surveillance subject of the measures taken […].

361. Furthermore, in the Court's view, a system of ex post facto review that does not produce

reasoned decisions in response to complaints submitted by individuals, or at least decisions that contain reasons accessible to security-cleared special counsel, is too dependent on the initiative and perseverance of appointed officials operating away from the public eye. With regard to the Swedish system, the Court notes that no details are communicated to the complainant as to the content and outcome of the investigation conducted by the Inspectorate and, hence, the Inspectorate seems to be afforded wide discretion. A reasoned decision has the undeniable advantage of providing publicly available guidance on the interpretation of the applicable legal rules, the limits to be observed and the manner in which the public interest and individual rights are to be balanced in the specific context of bulk interception of communications. […] These observations lead the Court to consider that the above-mentioned features of the Swedish system do not offer a sufficient basis for public confidence that abuses, if they occur, will be unveiled and remedied."

***Breyer v Germany*, App No 50001/12, Judgment, European Court of Human Rights (30 January 2020)**

107. The Court considers that the possibility of supervision by the competent data protection authorities ensures review by an independent authority. Moreover, since anyone, who believes his or her rights have been infringed, can lodge an appeal, the lack of notification and confidentiality of the retrieval procedure does not raise an issue under the Convention.

***Liblik and Others v Estonia*, Apps Nos 173/15 and 5 others, Judgment, European Court of Human Rights (28 May 2019)**

130. In this connection, the Court has emphasised the need for safeguards. In view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist guarantees against abuse which are adequate and effective. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law (see *Roman Zakharov*, cited above, § 232). Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights (see *Roman Zakharov*, cited above, § 233).

***Ivashchenko v Russia*, App No 61064/10, Judgment, European Court of Human Rights (13 February 2018)**

87. In situations when a person is at customs after *arriving* in the country (*a fortiori*, through such ports of entry as customs points for vehicles or those arriving on foot, as in the present case), bearing in mind the margin of appreciation afforded to the respondent State in the customs context, it is particularly pertinent to ascertain whether *post factum* judicial remedies were available and provided adequate v. […]"

***Zubkov and others v Russia*, App No 29431/05 and 2 others, Judgment, European Court of Human Rights (7 November 2017)**

129. It is also significant that the applicants' ability to challenge the legal and factual grounds for ordering surveillance measures against them was undermined by the refusal of access to the surveillance authorisations. The Court notes in this connection that there may be good reasons to keep a covert surveillance authorisation, or some parts of it, secret from its subject even after he or

she has become aware of its existence. Indeed, a full disclosure of the authorisation may in some cases reveal the working methods and fields of operation of the police or intelligence services and even possibly to identify their agents. At the same time, the information contained in decisions authorising covert surveillance might be critical for the person's ability to bring legal proceedings to challenge the legal and factual grounds for authorising covert surveillance. Accordingly, in the Court's opinion, when dealing with a request for the disclosure of a covert surveillance authorisation, the domestic courts are required to ensure a proper balance of the interests of the surveillance subject and the public interests. The surveillance subject should be granted access to the documents in question, unless there are compelling concerns to prevent such a decision.

130. In the present case, in response to the applicants' requests for access to the judicial decisions authorising covert surveillance measures against them, the domestic authorities referred to the documents' confidentiality as the sole reason for refusal of access. They did not carry out any balancing exercise between the applicants' interests and those of the public, and did not specify why disclosure of the surveillance authorisations, after the surveillance had stopped and the audio and video recordings had already been disclosed to the applicants, would have jeopardised the effective administration of justice or any other legitimate public interests.

131. The Court notes that the State agency performing the surveillance activities was to have exclusive possession of the judicial authorisations, which were to be held in respective operational-search files. There is no evidence that the domestic courts that examined the applicants' complaints about the covert surveillance had access to the classified material in the applicants' operational-search files and verified that the judicial authorisations to which the investigating authorities referred indeed existed and were part of the files, whether there had been relevant and sufficient reasons for authorising covert surveillance or whether the investigating authorities, while carrying out the surveillance, had complied with the terms of the judicial authorisations. The domestic courts did not, therefore, carry out an effective judicial review of the lawfulness and "necessity in a democratic society" of the contested surveillance measures and failed to furnish sufficient safeguards against arbitrariness within the meaning of Article 8 § 2 of the Convention.

132. […] Moreover, the refusal to disclose the surveillance authorisations to the applicants without any valid reason deprived them of any possibility to have the lawfulness of the measure, and its "necessity in a democratic society", reviewed by an independent tribunal in the light of the relevant principles of Article 8 of the Convention.

***Aycaguer v France*, App No 8806/12, Judgment, European Court of Human Rights (22 June 2017)**

3. Furthermore, as regards the deletion procedure, it is not disputed that access to such a procedure is only authorised for suspects, and not for convicted persons such as the applicant. The Court considers that convicted persons should also be given a practical means of lodging a request for the deletion of registered data (*B.B.*, cited above, § 68, and *Brunet*, cited above, §§ 41-43). That remedy should be made available, as it has previously pointed out, in order to ensure that the data storage period is proportionate to the nature of the offences and the aims of the restrictions (see paragraph 37 above; cf., *mutatis mutandis*, *Peruzzo and Martens v. Germany* (dec.), nos. 7841/08 and 57900/12, § 44, 4 June 2013, as well as *B.B.* and *M.B.*, cited above, §§ 62 and 54 respectively).

***Szabó and Vissy v Hungary*, App No 37138/14, Judgment, European Court of Human Rights (12 January 2016)**

33. […] in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them, the Court has accepted that, under certain circumstances, an individual may claim to be a victim on account of the mere existence of legislation permitting secret surveillance, even if he cannot point to any concrete measures specifically affecting him.

36. Most recently, the Court adopted, in *Roman Zakharov v. Russia*, a harmonised approach based on Kennedy, according to which firstly the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affect all users of communication services by instituting a system where any person can have his or her communications intercepted; and secondly the Court will take into account the availability or remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies.

37. The Court observes that the present applicants complained of an interference with their homes, communications and privacy on the basis of the very existence of the law permitting secret surveillance and the lack of adequate safeguards, admitting that their personal or professional situations were not of the kind that might normally attract the application of surveillance measures. They nevertheless thought they were at particular risk of having their communications intercepted as a result of their employment with civil-society organisations criticising the Government.

38. The Court observes that affiliation with a civil-society organisation does not fall within the grounds listed in section 7/E (1) point (a) sub-point (ad) and point (e) of the Police Act, which concern in essence terrorist threats and rescue operations to the benefit of Hungarian citizens in dangerous situations abroad. Nevertheless, it appears that under these provisions any person within Hungary may have his communications intercepted if interception is deemed necessary on one of the grounds enumerated in the law. The Court considers that it cannot be excluded that the applicants are at risk of being subjected to such measures should the authorities perceive that to do so might be of use to pre-empt or avert a threat foreseen by the legislation – especially since the law contains the notion of "persons concerned identified ... as a range of persons" which might include indeed any person. The Court also notes that, by examining their constitutional complaint on the merits, the Constitutional Court implicitly acknowledged the applicants' being personally affected by the legislation in question for the purposes of section 26(1) of the Act on the Constitutional Court. It is of importance at this juncture to note that they are staff members of a watchdog organisation, whose activities have previously been found similar, in some ways, to those of journalists. The Court accepts the applicants' suggestion that any fear of being subjected to secret surveillance might have an impact on such activities. In any case, whether or not the applicants belong to a targeted group, the Court considers that the legislation directly affects all users of communication systems and all homes.

39. Considering in addition that the domestic law does not appear to provide any possibility for an individual who alleges interception of his or her communications to lodge a complaint with an independent body, the Court is of the view that the applicants can claim to be victims of a violation of their rights under the Convention, within the meaning of Article 34 of the Convention. [...]

82. The Court notes at this juncture the liability of the executive to give account, in general terms rather than concerning any individual cases, of such operations to a parliamentary committee. However, it cannot identify any provisions in Hungarian legislation permitting a remedy granted by this procedure during the application of measures of secret surveillance to those who are subjected to secret surveillance but, by necessity, are kept unaware thereof. The Minister is under an obligation to present a general report, at least twice a year, to the responsible parliamentary committee about the functioning of national security services, which report, however, does not seem to be available to the public and by this appears to fall short of securing adequate safeguards in terms of public scrutiny. The committee is entitled, of its own motion, to request information from the Minister and the directors of the services about the activities of the national security services. However, the Court is not persuaded that this scrutiny is able to provide redress to any individual grievances caused by secret surveillance or to control effectively, that is, in a manner with a bearing on the operations themselves, the daily functioning of the surveillance organs, especially since it does not appear that the committee has access in detail to relevant documents. The scope of their supervision is therefore

limited.

86. Moreover, the Court has held that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned. In Hungarian law, however, no notification, of any kind, of the measures is foreseen. This fact, coupled with the absence of any formal remedies in case of abuse, indicates that the legislation falls short of securing adequate safeguards.

87. It should be added that although the Constitutional Court held that various provisions in the domestic law read in conjunction secured sufficient safeguards for data storage, processing and deletion, special reference was made to the importance of individual complaints made in this context. For the Court, the latter procedure is hardly conceivable, since once more it transpires from the legislation that the persons concerned will not be notified of the application of secret surveillance to them.

89. In total sum, the Court is not convinced that the Hungarian legislation on "section 7/E (3) surveillance" provides safeguards sufficiently precise, effective and comprehensive on the ordering, execution and potential redressing of such measures. Given that the scope of the measures could include virtually anyone, that the ordering is taking place entirely within the realm of the executive and without an assessment of strict necessity, that new technologies enable the Government to intercept masses of data easily concerning even persons outside the original range of operation, and given the absence of any effective remedial measures, let alone judicial ones, the Court concludes that there has been a violation of Article 8 of the Convention."

***Roman Zakharov v Russia*, App No 47143/06, Judgment, European Court of Human Rights (4 December 2015)**

164. The Court has consistently held in its case-law that the Convention does not provide for the institution of an *actio popularis* and that its task is not normally to review the relevant law and practice *in abstracto*, but to determine whether the manner in which they were applied to, or affected, the applicant gave rise to a violation of the Convention. Accordingly, in order to be able to lodge an application in accordance with Article 34, an individual must be able to show that he or she was "directly affected" by the measure complained of. This is indispensable for putting the protection mechanism of the Convention into motion, although this criterion is not to be applied in a rigid, mechanical and inflexible way throughout the proceedings.

165. Thus, the Court has permitted general challenges to the relevant legislative regime in the sphere of secret surveillance in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them. In the case of *Klass and Others v. Germany* the Court held that an individual might, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures had been in fact applied to him. The relevant conditions were to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures. […]

166. Following the *Klass and Others* case, the case-law of the Convention organs developed two parallel approaches to victim status in secret surveillance cases.

167. In several cases the Commission and the Court held that the test in *Klass and Others* could not

be interpreted so broadly as to encompass every person in the respondent State who feared that the security services might have compiled information about him or her. An applicant could not, however, be reasonably expected to prove that information concerning his or her private life had been compiled and retained. It was sufficient, in the area of secret measures, that the existence of practices permitting secret surveillance be established and that there was a reasonable likelihood that the security services had compiled and retained information concerning his or her private life [...]

168. In other cases the Court reiterated the *Klass and Others* approach that the mere existence of laws and practices which permitted and established a system for effecting secret surveillance of communications entailed a threat of surveillance for all those to whom the legislation might be applied. This threat necessarily affected freedom of communication between users of the telecommunications services and thereby amounted in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them. […]

169. Finally, in its most recent case on the subject, *Kennedy v. the United Kingdom*, the Court held that sight should not be lost of the special reasons justifying the Court's departure, in cases concerning secret measures, from its general approach which denies individuals the right to challenge a law in abstracto. The principal reason was to ensure that the secrecy of such measures did not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities and the Court. In order to assess, in a particular case, whether an individual can claim an interference as a result of the mere existence of legislation permitting secret surveillance measures, the Court must have regard to the availability of any remedies at the national level and the risk of secret surveillance measures being applied to him or her. Where there is no possibility of challenging the alleged application of secret surveillance measures at domestic level, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such cases, even where the actual risk of surveillance is low, there is a greater need for scrutiny by this Court.

170. The Court considers, against this background, that it is necessary to clarify the conditions under which an applicant can claim to be the victim of a violation of Article 8 without having to prove that secret surveillance measures had in fact been applied to him, so that a uniform and foreseeable approach may be adopted.

171. In the Court's view the *Kennedy* approach is best tailored to the need to ensure that the secrecy of surveillance measures does not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities and of the Court. Accordingly, the Court accepts that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies. As the Court underlined in *Kennedy*, where the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court and an exception to the rule, which denies individuals the right to challenge a law *in abstracto,* is justified. In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such

cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures.

172. The *Kennedy* approach therefore provides the Court with the requisite degree of flexibility to deal with a variety of situations which might arise in the context of secret surveillance, taking into account the particularities of the legal systems in the member States, namely the available remedies, as well as the different personal situations of applicants. […]

173. The Court notes that the contested legislation institutes a system of secret surveillance under which any person using mobile telephone services of Russian providers can have his or her mobile telephone communications intercepted, without ever being notified of the surveillance. To that extent, the legislation in question directly affects all users of these mobile telephone services.

174. Furthermore, for the reasons set out below, Russian law does not provide for effective remedies for a person who suspects that he or she was subjected to secret surveillance.

175. In view of the above finding, the applicant does not need to demonstrate that, due to his personal situation, he is at risk of being subjected to secret surveillance.

176. Having regard to the secret nature of the surveillance measures provided for by the contested legislation, the broad scope of their application, affecting all users of mobile telephone communications, and the lack of effective means to challenge the alleged application of secret surveillance measures at domestic level, the Court considers an examination of the relevant legislation *in abstracto* to be justified.

177. The Court therefore finds that the applicant is entitled to claim to be the victim of a violation of the Convention, even though he is unable to allege that he has been subject to a concrete measure of surveillance in support of his application. For the same reasons, the mere existence of the contested legislation amounts in itself to an interference with the exercise of his rights under Article 8. The Court therefore dismisses the Government's objection concerning the applicant's lack of victim status [...]

233. Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure.

234. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an

interception of his communications."

286. The Court will now turn to the issue of notification of interception of communications which is inextricably linked to the effectiveness of remedies before the courts.

287. It may not be feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. Therefore, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not "necessary in a democratic society", as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned. The Court also takes note of the Recommendation of the Committee of Ministers regulating the use of personal data in the police sector, which provides that where data concerning an individual have been collected and stored without his or her knowledge, and unless the data are deleted, he or she should be informed, where practicable, that information is held about him or her as soon as the object of the police activities is no longer likely to be prejudiced.

288. In the cases of *Klass and Others* and *Weber and Saravia* the Court examined German legislation which provided for notification of surveillance as soon as that could be done after its termination without jeopardising its purpose. The Court took into account that it was an independent authority, the G10 Commission, which had the power to decide whether an individual being monitored was to be notified of a surveillance measure. The Court found that the provision in question ensured an effective notification mechanism which contributed to keeping the interference with the secrecy of telecommunications within the limits of what was necessary to achieve the legitimate aims pursued. In the cases of *Association for European Integration and Human Rights and Ekimdzhiev and Dumitru Popescu (no 2),* the Court found that the absence of a requirement to notify the subject of interception at any point was incompatible with the Convention, in that it deprived the interception subject of an opportunity to seek redress for unlawful interferences with his or her Article 8 rights and rendered the remedies available under the national law theoretical and illusory rather than practical and effective. The national law thus eschewed an important safeguard against the improper use of special means of surveillance. By contrast, in the case of *Kennedy* the absence of a requirement to notify the subject of interception at any point in time was compatible with the Convention, because in the United Kingdom any person who suspected that his communications were being or had been intercepted could apply to the Investigatory Powers Tribunal, whose jurisdiction did not depend on notification to the interception subject that there had been an interception of his or her communications.

289. Turning now to the circumstances of the present case, the Court observes that in Russia persons whose communications have been intercepted are not notified of this fact at any point or under any circumstances. It follows that, unless criminal proceedings have been opened against the interception subject and the intercepted data have been used in evidence, or unless there has been a leak, the person concerned is unlikely ever to find out if his or her communications have been intercepted.

290. The Court takes note of the fact that a person who has somehow learned that his or her communications have been intercepted may request information about the corresponding data. It is worth noting in this connection that in order to be entitled to lodge such a request the person must be in possession of the facts of the operational search measures to which he or she was subjected. It follows that the access to information is conditional on the person's ability to prove that his or her

communications were intercepted. Furthermore, the interception subject is not entitled to obtain access to documents relating to interception of his or her communications; he or she is at best entitled to receive "information" about the collected data. Such information is provided only in very limited circumstances, namely if the person's guilt has not been proved in accordance with the procedure prescribed by law, that is, he or she has not been charged or the charges have been dropped on the ground that the alleged offence was not committed or that one or more elements of a criminal offence were missing. It is also significant that only information that does not contain State secrets may be disclosed to the interception subject and that under Russian law information about the facilities used in operational search activities, the methods employed, the officials involved and the data collected constitutes a State secret. In view of the above features of Russian law, the possibility to obtain information about interceptions appears to be ineffective.

291. The Court will bear the above factors – the absence of notification and the lack of an effective possibility to request and obtain information about interceptions from the authorities in mind when assessing the effectiveness of remedies available under Russian law.

292. Russian law provides that a person claiming that his or her rights have been or are being violated by a State official performing operational search activities may complain to the official's superior, a prosecutor or a court. The Court reiterates that a hierarchical appeal to a direct supervisor of the authority whose actions are being challenged does not meet the requisite standards of independence needed to constitute sufficient protection against the abuse of authority. A prosecutor also lacks independence and has a limited scope of review, as demonstrated above. It remains to be ascertained whether a complaint to a court may be regarded as an effective remedy [...]

294. […] Given that the Government did not submit any examples of domestic practice on examination of cassation appeals, the Court has strong doubts as to the existence of a right to lodge a cassation appeal against a judicial decision authorising interception of communications. At the same time, the interception subject is clearly entitled to lodge a supervisory review complaint however, in order to lodge a supervisory review complaint against the judicial decision authorising interception of communications, the person concerned must be aware that such a decision exists. Although the Constitutional Court has held that it is not necessary to attach a copy of the contested judicial decision to the supervisory review complaint, it is difficult to imagine how a person can lodge such a complaint without having at least the minimum information about the decision he or she is challenging, such as its date and the court which has issued it. In the absence of notification of surveillance measures under Russian law, an individual would hardly ever be able to obtain that information unless it were to be disclosed in the context of criminal proceedings against him or her or there was some indiscretion which resulted in disclosure [...]

298. The Court concludes from the above that the remedies referred to by the Government are available only to persons who are in possession of information about the interception of their communications. Their effectiveness is therefore undermined by the absence of a requirement to notify the subject of interception at any point, or an adequate possibility to request and obtain information about interceptions from the authorities. Accordingly, the Court finds that Russian law does not provide for an effective judicial remedy against secret surveillance measures in cases where no criminal proceedings were brought against the interception subject. It is not the Court's task in the present case to decide whether these remedies will be effective in cases where an individual learns about the interception of his or her communications in the course of criminal proceedings against him or her. […]

300. In view of the above considerations, the Court finds that Russian law does not provide for effective remedies to a person who suspects that he or she has been subjected to secret surveillance. By depriving the subject of interception of the effective possibility of challenging interceptions retrospectively, Russian law thus eschews an important safeguard against the improper use of secret surveillance measures."

***Dragojević v Croatia*, App No 68955/11, Judgment, European Court of Human Rights (15 January 2015)**

99. [There is no adequate and sufficient safeguards against abuse] in cases where the only effective possibility for an individual subjected to covert surveillance in the context of criminal proceedings is to challenge the lawfulness of the use of such measures before the criminal courts during the criminal proceedings against him or her. The Court has already held that although the courts could, in the criminal proceedings, consider questions of the fairness of admitting the evidence in the criminal proceedings, it was not open to them to deal with the substance of the Convention complaint that the interference with the applicant's right to respect for his private life was not "in accordance with the law"; still less was it open to them to grant appropriate relief in connection with the complaint.

100. This can accordingly be observed in the present case, where the competent criminal courts limited their assessment of the use of secret surveillance to the extent relevant to the admissibility of the evidence thus obtained, without going into the substance of the Convention requirements concerning the allegations of arbitrary interference with the applicant's Article 8 rights. At the same time, the Government have not provided any information on remedies – such as an application for a declaratory Judgment or an action for damages – which may become available to a person in the applicant's situation.

***Kennedy v The United Kingdom*, App No 26839/05, Judgment, European Court of Human Rights (18 May 2010)**

126. The applicant has alleged that the fact that calls were not put through to him and that he received hoax calls demonstrates a reasonable likelihood that his communications are being intercepted. The Court disagrees that such allegations are sufficient to support the applicant's contention that his communications have been intercepted. Accordingly, it concludes that the applicant has failed to demonstrate a reasonable likelihood that there was actual interception in his case.

127. Insofar as the applicant complains about the RIPA regime itself, the Court observes, first, that the RIPA provisions allow any individual who alleges interception of his communications to lodge a complaint with an independent tribunal, a possibility which was taken up by the applicant. The IPT concluded that no unlawful, within the meaning of RIPA, interception had taken place.

128. As to whether a particular risk of surveillance arises in the applicant's case, the Court notes that under the provisions of RIPA on internal communications, any person within the United Kingdom may have his communications intercepted if interception is deemed necessary on one or more of the grounds listed in section 5(3). The applicant has alleged that he is at particular risk of having his communications intercepted as a result of his high-profile murder case, in which he made allegations of police impropriety, and his subsequent campaigning against miscarriages of justice. The Court observes that neither of these reasons would appear to fall within the grounds listed in section 5(3) RIPA. However, in light of the applicant's allegations that any interception is taking place without lawful basis in order to intimidate him, the Court considers that it cannot be excluded that secret surveillance measures were applied to him or that he was, at the material time, potentially at risk of being subjected to such measures.

***Iordachi and Others v Moldova*, App No 25198/02, Judgment, European Court of Human Rights (10 February 2009)**

31. The Court notes that under the Operational Investigative Activities Act the authorities are authorised to intercept communications of certain categories of persons provided for in section 6 of that Act. In their capacity as human rights lawyers the applicants represent and thus have extensive contact with such persons […].

33. [...] the Court considers that it cannot be excluded that secret surveillance measures were applied to the applicants or that they were at the material time potentially at risk of being subjected to such measures.

34. The mere existence of the legislation entails, for all those who might fall within its reach, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunications services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for correspondence.

***Liberty and Others v The United Kingdom*, App No 58243/00, Judgment, European Court of Human Rights (1 July 2008)**

56. Telephone, facsimile and e-mail communications are covered by the notions of "private life" and "correspondence" within the meaning of Article 8. The Court recalls its findings in previous cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them.

57. The Court notes that the Government are prepared to proceed, for the purposes of the present application, on the basis that the applicants can claim to be victims of an interference with their communications sent to or from their offices in the United Kingdom and Ireland. In any event, under Section 3(2) the 1985 Act, the authorities were authorised to capture communications contained within the scope of a warrant issued by the Secretary of State and to listen to and examine communications falling within the terms of a certificate, also issued by the Secretary of State. Under section 6 of the 1985 Act arrangements had to be made regulating the disclosure, copying and storage of intercepted material. The Court considers that the existence of these powers, particularly those permitting the examination, use and storage of intercepted communications constituted an interference with the Article 8 rights of the applicants, since they were persons to whom these powers might have been applied.

***Weber and Saravia v Germany*, App No 54934/00, Decision, European Court of Human Rights (29 June 2006)**

78. The Court further notes that the applicants, even though they were members of a group of persons who were likely to be affected by measures of interception, were unable to demonstrate that the impugned measures had actually been applied to them. It reiterates, however, its findings in comparable cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them. […]

135. The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively. However, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not "necessary in a democracy society", as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. Indeed, such notification might reveal the working methods and fields of operation of the Intelligence Service. As soon as notification can be carried out without

jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned.

***Rotaru v Romania*, App No 28341/95, Judgment, European Court of Human Rights (4 May 2000)**

35. The Court reiterates, as to the concept of victim, that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him. Furthermore, "a decision or measure favourable to the applicant is not in principle sufficient to deprive him of his status as a 'victim' unless the national authorities have acknowledged, either expressly or in substance, and then afforded redress for, the breach of the Convention".

36. In the instant case the Court notes that the applicant complained of the holding of a secret register containing information about him, whose existence was publicly revealed during judicial proceedings. It considers that he may on that account claim to be the victim of a violation of the Convention... Assuming that it may be considered that [the 25 November 1997 Judgment of the Bucharest Court of Appeal] did, to some extent, afford the applicant redress for the existence in his file of information that proved false, the Court takes the view that such redress is only partial and that at all events it is insufficient under the case-law to deprive him of his status of victim. […]

***Malone v The United Kingdom*, App No 8691/79, Judgment, European Court of Human Rights (2 August 1984)**

64. Despite the applicant's allegations, the Government have consistently declined to disclose to what extent, if at all, his telephone calls and mail have been intercepted otherwise on behalf of the police. [...]

86. The applicant, as a suspected receiver of stolen goods, was, it may be presumed, a member of a class of persons potentially liable to be directly affected by this practice. The applicant can therefore claim, for the purposes of Article 25 (art. 25) of the Convention, to be a "victim" of a violation of Article 8 (art. 8) by reason of the very existence of this practice, quite apart from any concrete measure of implementation taken against. This remains so despite the clarification by the Government that in fact the police had neither caused his telephone to be metered nor undertaken any search operations on the basis of any list of telephone numbers obtained from metering.

***Klass and Others v Germany*, App No 5029/71, Judgment, European Court of Human Rights (6 September 1978)**

34. […] the question arises in the present proceedings whether an individual is to be deprived of the opportunity of lodging an application with the Commission because, owing to the secrecy of the measures objected to, he cannot point to any concrete measure specifically affecting him. In the Court's view, the effectiveness (l'effet utile) of the Convention implies in such circumstances some possibility of having access to the Commission. If this were not so, the efficiency of the Convention's enforcement machinery would be materially weakened. The procedural provisions of the Convention must, in view of the fact that the Convention and its institutions were set up to protect the individual, be applied in a manner which serves to make the system of individual applications efficacious. The Court therefore accepts that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him. The relevant conditions are to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures [...]

36. The Court points out that where a State institutes secret surveillance the existence of which

remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 could to a large extent be reduced to a nullity. It is possible in such a situation for an individual to be treated in a manner contrary to Article 8, or even to be deprived of the right granted by that Article, without his being aware of it and therefore without being able to obtain a remedy either at the national level or before the Convention institutions [...] The Court finds it unacceptable that the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation. A right of recourse to the Commission for persons potentially affected by secret surveillance is to be derived from Article 25, since otherwise Article 8 runs the risk of being nullified.

41. […] Although telephone conversations are not expressly mentioned in paragraph 1 of Article 8, the Court considers, as did the Commission, that such conversations are covered by the notions of "private life" and "correspondence" referred to by this provision. […]
Neither before the Commission nor before the Court did the Government contest this issue. Clearly, any of the permitted surveillance measures, once applied to a given individual, would result in an interference by a public authority with the exercise of that individual's right to respect for his private and family life and his correspondence. Furthermore, in the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for private and family life and for correspondence. The Court does not exclude that the contested legislation, and therefore the measures permitted thereunder, could also involve an interference with the exercise of a person's right to respect for his home. However, the Court does not deem it necessary in the present proceedings to decide this point. […]

57. As regards review a posteriori, it is necessary to determine whether judicial control, in particular with the individual's participation, should continue to be excluded even after surveillance has ceased. Inextricably linked to this issue is the question of subsequent notification, since there is in principle little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality. The applicants' main complaint under Article 8 (art. 8) is in fact that the person concerned is not always subsequently informed after the suspension of surveillance and is not therefore in a position to seek an effective remedy before the courts. Their preoccupation is the danger of measures being improperly implemented without the individual knowing or being able to verify the extent to which his rights have been interfered with. In their view, effective control by the courts after the suspension of surveillance measures is necessary in a democratic society to ensure against abuses; otherwise adequate control of secret surveillance is lacking and the right conferred on individuals under Article 8 (art. 8) is simply eliminated. In the Government's view, the subsequent notification which must be given since the Federal Constitutional Court's Judgment corresponds to the requirements of Article 8 para. 2 (art. 8-2). In their submission, the whole efficacy of secret surveillance requires that, both before and after the event, information cannot be divulged if thereby the purpose of the investigation is, or would be retrospectively, thwarted. They stressed that recourse to the courts is no longer excluded after notification has been given, various legal remedies then becoming available to allow the individual, inter alia, to seek redress for any injury suffered.

58. In the opinion of the Court, it has to be ascertained whether it is even feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, as the Federal Constitutional Court rightly observed, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. In the Court's view, in so far as the "interference" resulting from the contested legislation is in principle justified under Article 8 para. 2 (art. 8-2), the fact of not informing the individual once surveillance has

ceased cannot itself be incompatible with this provision since it is this very fact which ensures the efficacy of the "interference". Moreover, it is to be recalled that, in pursuance of the Federal Constitutional Court's Judgment of 15 December 1970, the person concerned must be informed after the termination of the surveillance measures as soon as notification can be made without jeopardising the purpose of the restriction."

African Commission on Human and Peoples' Rights, Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa, ACHPR/Res.573 (LXXVII) (9 November 2023)

The African Commission calls on States Parties to: v. Ensure that victims of violations arising from arbitrary surveillance measures have access to effective remedies and take specific measures to investigate and prosecute cases of illegal and indiscriminate surveillance.

***V.S. v Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost,* (C-205/21), Judgment, Court of Justice of the European Union (26 January 2023)**

64. Second, the scope of the requirement laid down in Article 10(a) of Directive 2016/680 that the processing of the personal data must have been 'authorised by Union or Member State law' must be determined in the light of the requirement enshrined in Article 52(1) of the Charter that any limitation on the exercise of a fundamental right must be 'provided for by law'.

65. In that regard, it is clear from the Court's case-law that that requirement means that the legal basis authorising such a limitation must define the scope of that limitation sufficiently clearly and precisely (see, to that effect, judgment of 6 October 2020, État luxembourgeois (Right to bring an action against a request for information in tax matters), C-245/19 and C-246/19, EU:C:2020:795, paragraph 76 and the case-law cited).

66. Furthermore, it follows from the case-law recalled in the previous paragraph of the present judgment that there can be no uncertainty as to the provisions of EU law pursuant to which national law may authorise processing of biometric and genetic data, such as the processing at issue in the main proceedings, or as to the applicable conditions governing that authorisation. Data subjects and the courts having jurisdiction must be in a position to be able to determine precisely, in particular, the conditions under which that processing may take place and the purposes which it may lawfully pursue. However, the rules of the GDPR and those of the directive that are applicable to those requirements may differ.

76. In the light of the foregoing, the answer to the first and second questions is that Article 10(a) of Directive 2016/680, read in the light of Article 52 of the Charter, must be interpreted as meaning that the processing of biometric and genetic data by the police authorities with a view to their investigative activities, for purposes of combating crime and maintaining law and order, is authorised by Member State law, within the meaning of Article 10(a) of Directive 2016/680, provided that the law of that Member State contains a sufficiently clear and precise legal basis to authorise that processing. The fact that the national legislative act containing such a legal basis refers, furthermore, to the GDPR, and not to Directive 2016/680, is not capable, in itself, of calling the existence of such authorisation into question, provided that it is apparent, in a sufficiently clear, precise and unequivocal manner, from the interpretation of the set of applicable provisions of national law that the processing of biometric and genetic data at issue falls within the scope of that directive, and not of that regulation.

77. By its third question, the referring court asks, in essence, whether Article 6(a) of Directive 2016/680 and Articles 47 and 48 of the Charter must be interpreted as precluding national legislation which provides that, if the person accused of an intentional offence subject to public prosecution refuses to cooperate voluntarily in the collection of the biometric and genetic data concerning him or her in order for them to be entered in a record, the criminal court having jurisdiction must authorise enforcement of their collection, without having the power to assess whether there are serious

grounds for believing that the person concerned has committed the offence of which he or she is accused.

86. It follows from all the foregoing that Article 6(a) of Directive 2016/680 does not preclude national legislation which provides for the compulsory collection, in order to be entered in a record, of biometric and genetic data concerning persons in respect of whom sufficient evidence is gathered that they are guilty of an intentional offence subject to public prosecution and who have been accused for that reason.

88. Consequently, any accused person who has opposed the collection of photographic, dactyloscopic and genetic data concerning him or her in the context of a procedure such as the creation of a police record, a procedure which has to comply with the requirements of Article 10 of Directive 2016/680, must, as Article 47 of the Charter requires, be able to enjoy the right to an effective remedy before a tribunal against the decision to authorise enforcement of their collection, for the purpose of relying on the rights which he or she derives from the safeguards laid down by that provision and, in particular, from the safeguard under Article 10(a) of the directive that collection of the biometric and genetic data must be carried out in compliance with the national legislation that authorises collection. In particular, that safeguard entails the court with jurisdiction having the ability to verify that the measure accusing the person concerned that constitutes the legal basis for the creation of the police record has been adopted – in accordance with the rules of national criminal procedure – in the light of sufficient evidence that he or she is guilty of an intentional offence subject to public prosecution.

101. It follows from all the foregoing that Article 47 of the Charter does not preclude a national court, when it rules on an application for authorisation of enforcement of the collection of biometric and genetic data of an accused person in order for them to be entered in a record, from being unable to assess the evidence on which the accusation of that person is based, provided that national law subsequently guarantees effective judicial review of the conditions for that accusation, from which the authorisation to collect those data arises.

107. The fact that the court which must make such a judicial decision cannot assess, at that stage of the criminal procedure, whether the evidence on which the accusation of the person concerned is based is sufficient constitutes a guarantee for the latter of observance of the right to be presumed innocent.

108. Such a guarantee is all the more necessary where national law, such as the provision at issue in the main proceedings, provides that the court having jurisdiction to rule on enforcement of collection of the biometric and genetic data concerning accused persons in order for them to be entered in a record is the court which, at the judicial stage of the criminal procedure, will have to rule on the criminal liability of such a person. Observance of the right to be presumed innocent requires that court to be free of any bias and any prejudice when it carries out that examination (see, to that effect, judgment of 16 November 2021, *Prokuratura Rejonowa w Mińsku Mazowieckim and Others*, C-748/19 to C-754/19, EU:C:2021:931, paragraph 88).

109. It follows from the foregoing that the right to be presumed innocent, enshrined in Article 48 of the Charter, does not preclude accused persons, at the preliminary stage of the criminal procedure, from being the subject of a measure by which the biometric and genetic data concerning them are collected in order to be entered in a record and which is authorised by a court that does not have the power to assess, at that stage, the evidence upon which such accusation is based.

110. It follows from all the foregoing that the answer to the third question is that Article 6(a) of Directive 2016/680 and Articles 47 and 48 of the Charter must be interpreted as not precluding national legislation which provides that, if the person accused of an intentional offence subject to public prosecution refuses to cooperate voluntarily in the collection of the biometric and genetic data concerning him or her in order for them to be entered in a record, the criminal court having jurisdiction

must authorise a measure enforcing their collection, without having the power to assess whether there are serious grounds for believing that the person concerned has committed the offence of which he or she is accused, provided that national law subsequently guarantees effective judicial review of the conditions for that accusation, from which the authorisation to collect those data arises.

***La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées; Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministers* (C-511/18, C-512/18 and C-520/18), Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2020)**

190. The competent national authorities undertaking real-time collection of traffic and location data must notify the persons concerned, in accordance with the applicable national procedures, to the extent that and as soon as that notification is no longer liable to jeopardise the tasks for which those authorities are responsible. That notification is, indeed, necessary to enable the persons affected to exercise their rights under Articles 7 and 8 of the Charter to request access to their personal data that has been the subject of those measures and, where appropriate, to have the latter rectified or erased, as well as to avail themselves, in accordance with the first paragraph of Article 47 of the Charter, of an effective remedy before a tribunal, that right indeed being explicitly guaranteed.

191. With regard to the notification required in the context of automated analysis of traffic and location data, the competent national authority is obliged to publish information of a general nature relating to that analysis without having to notify the persons concerned individually. However, if the data matches the parameters specified in the measure authorising automated analysis and that authority identifies the person concerned in order to analyse in greater depth the data concerning him or her, it is necessary to notify that person individually. That notification must, however, occur only to the extent that and as soon as it is no longer liable to jeopardise the tasks for which those authorities are responsible.

***Draft Agreement between Canada and the European Union on the Transfer of Passenger Name Record data* (1/15), Court of Justice of the European Union, Grand Chamber, Opinion pursuant to Article 218(11) TFEU (26 July 2017)**

224. [...] information must, in accordance with the case-law [...], be provided only once it is no longer liable to jeopardise the investigations being carried out by the government authorities referred to in the envisaged agreement.

225. The envisaged agreement should therefore specify that air passengers whose PNR data has been used and retained by the Canadian Competent Authority [...] and those whose data has been disclosed to other government authorities or to individuals, are to be notified, by that authority, of such use and such disclosure […]

226. As regards air passengers' right to redress, Article 14(2) of the envisaged agreement provides that Canada is to ensure that any individual who is of the view that their rights have been infringed by a decision or action in relation to their PNR data may seek effective judicial redress, in accordance with Canadian law, or such other remedy which may include compensation.

227. Since that provision refers to 'any individual who is of the view that their rights have been infringed', it covers all air passengers, regardless of their nationality, their residence, their domicile or their presence in Canada. Furthermore, it must, as the Council has observed, be understood as meaning that air passengers have a legal remedy before a tribunal […]

***Tele2 Sverige AB v Post- Och telestyrelsen* (C-203/15); *Secretary of State for the Home Department v Tom Watson et al.* (C-698/16), Joined Cases, Judgment, Grand Chamber, Court**

of Justice of the European Union (21 December 2016)

121. […] the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed.

IX. DUTY TO PROTECT AGAINST THIRD-PARTY INTERFERENCE AND ACCESS TO REMEDY

This sub-chapter focuses on the states' duty to protect against third-party interference with the right to privacy. It therefore does not contain references to statements by human rights mechanisms in relation to the obligations of business enterprises. The latter have been compiled in the sub-chapter dedicated to companies specifically.

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

10. Calls upon all States: (h) To develop or maintain and implement adequate legislation, with effective sanctions and remedies, that protects individuals against violations and abuses of the right to privacy, namely through the collection, processing, retention or use of personal data by individuals, Governments, business enterprises or private organizations without the individual's free, explicit and informed consent or unless otherwise unlawful, in accordance with international human rights law;

** See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019)*

UN Human Rights Committee, General Comment No 16: Article 17 (Right to Privacy), UN Doc HRI/GEN/1/Rev.1 (8 April 1988)

10. [...] Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant."

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

Noting that general comment No. 16 of the Human Rights Committee recommends that States take effective measures to prevent the unlawful retention, processing and use of personal data stored by public authorities and business enterprises,

** See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016)*

Report of the Special Rapporteur on the Promotion and Protection of Human Rights while Counter-Terrorism, Human Rights Implications of the Development, Use, Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism, UN Doc A/HRC/52/39 (1 March 2023)

56. The Special Rapporteur recommends that States: (c) Pass comprehensive domestic legislation which adequately protects the right to privacy as a gateway right enabling and sustaining the protection of other fundamental human rights, including non-derogable rights. This includes comprehensive data protection legislation;

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/17/27 (16 May 2011)

52. When a cyber-attack can be attributed to the State, it clearly constitutes *inter alia* a violation of its obligation to respect the right to freedom of opinion and expression. Although determining the origin of cyber-attacks and the identity of the perpetrator is often technically difficult, it should be noted that States have an obligation to protect individuals against interferences by third parties that undermines the enjoyment of the right to freedom of opinion and expression. This positive obligation to protect entails that States must take appropriate and effective measures to investigate actions taken by third parties, hold the persons responsible to account, and adopt measures to prevent such recurrence in the future.

Concluding Observations on the Seventh Periodic Report of Colombia, Human Rights Committee, UN Doc CCPR/C/COL/CO/7 (4 November 2016)

33. The State party should: […] (b) Adopt effective measures to prevent illegal surveillance activities from being conducted and ensure that all allegations regarding such illegal activities are investigated and that the responsible parties are held accountable for their acts;

***N.F. and Others v Russia*, Apps Nos 3537/15 and 8 others, Judgment, European Court of Human Rights (12 September 2023)**

51. In so far as the guarantees aimed at regulating access by third parties and protecting data integrity and confidentiality are concerned, the Court observes that under the Police Act, police must protect data in their care from illegal or accidental access, destruction, copying and dissemination. Such information may be provided to State authorities or officials only in cases defined by federal law (see "Relevant domestic law" above, paragraph 23). However, as noted above, the available regulations make no distinction as to the purpose and other important functionalities of retention and processing of such data, and thus give no real possibility to conduct a proportionality analysis with respect to possible access by third parties, in line with the requirements of Article 8.

***Uzun v Germany*, App No 35623/05, Judgment, European Court of Human Rights (2 September 2010)**

66. While the Court is not barred from gaining inspiration from these principles, it finds that these rather strict standards, set up and applied in the specific context of surveillance of telecommunications, are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations. It will therefore apply the more general principles on adequate protection against arbitrary interference with.

X. DUE DILIGENCE INCLUDING IMPACT ASSESSMENTS

UN General Assembly Resolution on the Promotion and Protection of Human Right in the Context of Digital Technologies, UN Doc A/RES/78/213 (19 December 2023)

20. *Calls upon* Member States and, where applicable, other stakeholders: (a) To conduct human rights due diligence, including regular, comprehensive human rights impact assessments of digital technologies, including artificial intelligence, throughout their life cycle, including their conception, design, development, deployment, use, sale, procurement or operation, in order to prevent and mitigate their adverse human rights impacts, and ensuring effective remedies as well as human oversight, accountability and legal responsibility;

UN Human Rights Council Resolution on New and Emerging Digital Technologies and Human Rights, UN Doc A/HRC/RES/53/29 (14 July 2023)

Highlighting further the importance of ensuring appropriate safeguards and human oversight in the application of new and emerging digital technologies, and of respecting and promoting human rights in national, regional and international regulatory frameworks and legislation, and on the conception, design, use, development, further deployment and impact assessments and technical standard-setting of new and emerging digital technologies while ensuring the meaningful participation of all relevant stakeholders, including the private sector, academia, the media and civil society,

3. *Highlights* the importance of the need to respect, protect and promote human rights and fundamental freedoms, in recognition of the inherent dignity of the human person, throughout the lifecycle of artificial intelligence systems and, towards this end, the need to pay particular attention to: (a) Protecting individuals from harm caused by artificial intelligence systems, including by ensuring the safety of artificial intelligence systems, introducing frameworks for impact assessments related to human rights, exercising due diligence to assess, prevent and mitigate adverse human rights impacts, and ensuring effective remedies and human oversight, accountability and legal responsibility;

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

56. […] OHCHR recommends that States: (b) Conduct human rights due diligence systematically, including regular comprehensive human rights impact assessments, when designing, developing, purchasing, deploying and operating surveillance systems;

Report of the United Nations High Commissioner for Human Rights, The right to Privacy in the Digital Age, UN Doc A/HRC/48/31 (13 September 2021)

48. States and businesses should ensure that comprehensive human rights due diligence is conducted when AI systems are acquired, developed, deployed and operated, as well as before big data held about individuals are shared or used. As well as resourcing and leading such processes, States may also require or otherwise incentivize companies to conduct comprehensive human rights due diligence. […]

60. The High Commissioner recommends that States and business enterprises: (a) Systematically conduct human rights due diligence throughout the life cycle of the AI systems they design, develop, deploy, sell, obtain or operate. A key element of their human rights due diligence should be regular, comprehensive human rights impact assessments […]

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and

Fundamental Freedoms While Countering Terrorism, Human Rights Impact of Counter-Terrorism and Countering (Violent) Extremism Policies and Practices on the Rights of Women, Girls and the Family, UN Doc A/HRC/46/36 (22 January 2021)

58. At both the domestic and international levels, Member States must ensure that border and immigration enforcement and administration are subject to binding legal obligations to prevent, combat and remedy racial and xenophobic discrimination in the design and use of digital border technologies. These obligations include but are not limited to: […] (b) An immediate moratorium on the procurement, sale, transfer and use of surveillance technology, until robust human rights safeguards are in place to regulate such practices. These safeguards include human rights due diligence that complies with international human rights law prohibitions on racial discrimination, independent oversight, strict privacy and data protection laws, and full transparency about the use of surveillance tools such as image recordings and facial recognition technology. In some cases, it will be necessary to impose outright bans on technology that cannot meet the standards enshrined in international human rights legal frameworks prohibiting racial discrimination;"

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

6. *Acknowledges* that the conception, design, use, deployment and further development of new and emerging technologies, such as those that involve artificial intelligence, may have an impact on the enjoyment of the right to privacy and other human rights, and that the risks to these rights can and should be avoided and minimized by adapting or adopting adequate regulation or other appropriate mechanisms, […]

**See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (16 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014)*

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)

Recognizing also the need to ensure that international human rights law is respected, including by conducting human rights impact assessments in the conception, design, development, deployment, evaluation, regulation and technical standard-setting of data- driven technologies, and to ensure that they are subject to adequate safeguards and oversight,

UN Human Rights Council Resolution on New and Emerging Digital Technologies and Human Rights, UN Doc A/HRC/RES/47/23 (13 July 2021)

Reiterating the importance of ensuring appropriate safeguards and human oversight in the application of new and emerging digital technologies, and of respecting and promoting human rights in national, regional and international regulatory frameworks and legislation and on the conception, design, use, development, further deployment and impact assessments of new and emerging digital technologies, while ensuring the meaningful participation of all relevant stakeholders, including the private sector, academia and civil society,

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

57. […] OHCHR recommends that States: (e) Establish robust well-tailored export control regimes applicable to surveillance technologies, the use of which carries high risks for the enjoyment of

human rights; States should require transparent human rights impact assessments that take into account the capacities of the technologies at issue as well as the situation in the recipient State, including compliance with human rights, adherence to the rule of law, the existence and effective enforcement of applicable laws regulating surveillance activities and the existence of independent oversight mechanisms;

Report of the Office of the United Nations High Commissioner for Human Rights, 'The practical application of the Guiding Principles on Business and Human Rights to the activities of technology companies', UN Doc A/HRC/50/56 (21 April 2022)

32. The requirement for companies to undertake human rights due diligence across their activities and business relationships to identify, prevent, mitigate and account for how they address the actual and potential human rights harms connected to their business activities is a central element of their corporate responsibility (guiding principle 17). The human rights due diligence requirement extends to a company's products and services. This is highly relevant when considering the impacts of digital technologies, as it is mostly in their use that human rights harms will manifest. […]

37. Human rights due diligence should be done with reference to all internationally recognized human rights (guiding principle 12, commentary). For many in the technology sector, questions will arise about the company's impacts on privacy and freedom of expression. However, there is already evidence that the use and misuse of technologies can have online and offline impacts on a wide range of other human rights. For example, the use of artificial intelligence tools by law enforcement and the criminal justice system could have an impact on an individual's right to be free from arbitrary arrest or to equality before the law; surveillance technologies could impact on the right to peaceful assembly; the use of social media platforms could impact the right to mental health; and property rental platforms could alter housing markets, possibly impacting the right to an adequate standard of living.

Report of the United Nations High Commissioner for Human Rights, The right to Privacy in the Digital Age, UN Doc A/HRC/48/31 (13 September 2021)

48. States and businesses should ensure that comprehensive human rights due diligence is conducted when AI systems are acquired, developed, deployed and operated, as well as before big data held about individuals are shared or used. As well as resourcing and leading such processes, States may also require or otherwise incentivize companies to conduct comprehensive human rights due diligence. […]

60. The High Commissioner recommends that States and business enterprises: (a) Systematically conduct human rights due diligence throughout the life cycle of the AI systems they design, develop, deploy, sell, obtain or operate. A key element of their human rights due diligence should be regular, comprehensive human rights impact assessments […]"

Report of the United Nations High Commissioner for Human Rights, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests, UN Doc A/HRC/44/24 (24 June 2020)

53. In this context, the High Commissioner recommends that States:
(j) Establish a moratorium on the use of facial recognition technology in the context of peaceful assemblies, at least until the authorities responsible can demonstrate compliance with privacy and data protection standards as well as the absence of significant accuracy issues and discriminatory impacts, and until the following recommendations are implemented:
(i) Systematically conduct human rights due diligence before deploying facial recognition technology devices and throughout the entire life cycle of the tools deployed;
(v) When relying on private companies to procure or deploy these facial recognition technologies, request that companies carry out human rights due diligence to identify, prevent,

mitigate and address potential and actual adverse impact on human rights and, in particular, ensure that data protection and non-discrimination requirements be included in the design and the implementation of these technologies

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

46. According to the Guiding Principles, all companies have a responsibility to undertake human rights due diligence to identify and address any human rights impacts of their activities. Taking a concrete example, companies selling surveillance technology should carry out, as part of their due diligence, a thorough human rights impact assessment prior to any potential transaction. Risk mitigation should include clear end-use assurances being stipulated in contractual agreements with strong human rights safeguards that prevent arbitrary or unlawful use of the technology and periodic reviews of the use of technology by States. Companies collecting and retaining user data need to assess the privacy risks connected to potential State requests for such data, including the legal and institutional environment of the States concerned. They must provide for adequate processes and safeguards to prevent and mitigate potential privacy and other human rights harms. Human rights impact assessments also need to be conducted, as part of the adoption of the terms of service and design and engineering choices that have implications for security and privacy, and decisions taken to provide or terminate services in a particular context (see A/HRC/32/38, para. 11).

47. […] In instances where national laws and regulations hinder such reporting, companies should use to the greatest extent possible any leverage they may have and are encouraged to advocate for the possibility to release such information.

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

44. Enterprises that provide content or Internet services, or supply the technology and equipment that make digital communications possible, for example, should adopt an explicit policy statement outlining their commitment to respect human rights throughout the company's activities. They should also have in place appropriate due diligence policies to identify, assess, prevent and mitigate any adverse impact. Companies should assess whether and how their terms of service, or their policies for gathering and sharing customer data, may result in an adverse impact on the human rights of their users.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

32. In short, companies have not disclosed instances of meaningful action, such as putting in place due diligence processes that identify and avoid causing or contributing to adverse human rights impacts through their own activities and that prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships (A/HRC/17/31, annex, principle 13) There is, for example, no public information suggesting that human rights assessments are a routine component of due diligence during sales, that companies give decisive weight to these assessments and that these assessments continue throughout the life cycle of the product and any contract for after-sales support. Indeed, mounting evidence of the industry's central role in facilitating gross human rights abuses, coupled with its steadfast refusal to explain its safeguards, makes it difficult to avoid the conclusion that such self-regulation lacks substance.

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, UN Doc A/HRC/41/41 (17 May 2019)

63. […] States should adopt and enforce laws and policies that focus on creating mandatory

requirements for digital technology companies to exercise due diligence to identify, prevent, mitigate, and account for how they address, human rights impacts of their business and products, as well as for robust transparency and remediation mechanisms. […]

Concluding Observations on the Sixth Periodic Report of Belgium, Human Rights Committee, UN Doc CCPR/C/BEL/CO/6 (6 December 2019)

12. The State party should: (a) Carry out an assessment of its legislation and practices for preventing and combating terrorism in respect of their compatibility with its obligations under the Covenant;

Commissioner for Human Rights, Council of Europe, Positions on Counter-Terrorism and Human Rights Protection, CommDH/PositionPaper(2015)1 (5 June 2015)

An independent assessment of the use and impact of individual information databases must be carried out in order to ensure that they are necessary and proportionate. The use of data collected through telecommunication surveillance or other forms of undercover investigations should be strictly limited to the purpose of investigating serious crimes. […]

SECTION 3: SAFEGUARDING CIVIC SPACES

In the introduction to this section, you may expect to find general references to the impact of surveillance measures on civic spaces. The section moves on to elaborate on the particular safeguards afforded by the human rights legal framework in relation to privileged communications. It first examines the protection of legal professional privilege, moving on to the protection of journalist sources, further looking into the protection of journalists and human rights defenders in light of the particular risks they are subjected to as a result of their profession and finally underlining the protection stemming from the freedom to peaceful assembly.

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN Doc A/78/520 (10 October 2023)

33. The ubiquity of sophisticated communications surveillance poses obvious threats to civil society actors' and organizations' rights to privacy and free expression, as well as such related rights as the freedom of assembly and association and the freedom to manifest one's religion. Many global study respondents reported experiences of digital surveillance and the transfer of their private data […], leading to deep concerns among civil society about permissive surveillance and data-sharing arrangements, and a dearth of regulation and due diligence with respect to both States and private companies. The lack of regulation for private cybersecurity firms is profoundly concerning. The pernicious effect of unchecked and unregulated surveillance on civil society has been vividly demonstrated in the field of spyware. The position paper of the Special Rapporteur on the global regulation of the counter-terrorism spyware technology trade sets out in detail the inadequacy of the existing regulatory regime and identifies the minimum features of a rights-respecting approach to the unique challenge of spyware.

Concluding Observations on the Second Periodic Report of Uganda, Human Rights Committee, UN Doc CCPR/C/UGA/CO/2 (20 July 2023)

41. The State party should ensure that adequate safeguards, including judicial review, are in place to guarantee that the extensive powers of search and surveillance at its disposal are exercised in full conformity with the Covenant, including powers provided under the Regulation of Interception of Communications Act, 2010. The State party should ensure that such powers are not abused to intimidate and suppress the activities of political opposition members, lawyers, journalists and human rights defenders, including powers to carry out warrantless searches under the Police Act. […]

Report of the Working Group on Enforced and Involuntary Disappearances, 'New technologies and enforced disappearances', UN Doc A/HRC/54/22/Add.5 (11 September 2023)

25. Instances as the one here described confirm the urgent need to develop more secure means that can ensure the exclusively humanitarian use of data and safe channels of communication for human rights defenders, civil society organizations, humanitarian actors, human rights bodies and relatives of disappeared persons. In the meantime, the use of available free applications that allow the secure collection, storage and analysis of data is a first mitigation measure to be put in place. The development of open source and easily accessible tools to perform reliable forensic analysis of devices that may have been compromised has also been mentioned as a relevant action to mitigate some of the risks described in this section. Moreover, many of the contributions received by the Working Group emphasized the importance of providing adequate training to members of civil

society organizations and relatives of disappeared persons to increase their awareness of risks related to new technologies and mitigate them, including through disseminating information on digital hygiene, data sensitivity, harm, and minimisation. These programmes should allow civil society organizations to integrate security methods in their work and acquire in-house capacity to diagnose existing risks and recover from threats or attacks.

Concluding Observations on the Initial Report of the State of Palestine, UN Doc CCPR/C/PSE/CO/1 (21 July 2023)

37. […] The Committee is also concerned about the lack of sufficient safeguards against arbitrary interference with the right to privacy in the form of surveillance, interception activities, access to personal data, and the diffusion of personal data with a view to discrediting opposition leaders, activists, and individuals on the basis of their gender, gender identity and sexual orientation. […]

Concluding Observations on the Sixth Periodic Report of Sri Lanka, Human Rights Committee, UN Doc CCPR/C/LKA/CO/6 (21 March 2023)

42. […]. It also regrets allegations of harassment and surveillance of members of civil society by the police and intelligence services (arts. 21, 22 and 26).

Concluding Observations on the Sixth Periodic Report of Morocco, Human Rights Committee, UN Doc CCPR/C/MAR/CO/6 (4 November 2016)

37. The Committee is concerned by reports of illegal infringements of the right to privacy in the course of surveillance operations conducted by law enforcement and intelligence agencies targeting journalists, human rights defenders and perceived opponents of the Government, particularly those located in Western Sahara.

A. PROFESSIONAL CONFIDENTIALITY AND PRIVILEGED COMMUNICATIONS – LEGAL PROFESSIONAL PRIVILEGE

***Saber v Norway*, App No 459/18, Judgment, European Court of Human Rights (17 December 2020)**

51. […] the Court has acknowledged the importance of specific procedural guarantees when it comes to protecting the confidentiality of exchanges between lawyers and their clients and of LPP (see, inter alia, *Sommer v. Germany*, no. 73607/13, § 56, 27 April 2017, and *Michaud v. France*, no. 12323/11, § 130, ECHR 2012). It has emphasised that professional secrecy is the basis of the relationship of trust existing between a lawyer and his client and that the safeguarding of professional secrecy is in particular the corollary of the right of a lawyer's client not to incriminate himself, which presupposes that the authorities seek to prove their case without resorting to evidence obtained through methods of coercion or oppression in defiance of the will of the "person charged" (see, for example, *André and Another v. France*, no. 18603/03, § 41, 24 July 2008). [….] Moreover, the Court has stressed that it is clearly in the general interest that any person who wishes to consult a lawyer should be free to do so under conditions which favour full and uninhibited discussion and that it is for that reason that the lawyer-client relationship is, in principle, privileged. It has not limited that consideration to matters relating to pending litigation only and has emphasised that, whether in the context of assistance for civil or criminal litigation or in the context of seeking general legal advice, individuals who consult a lawyer can reasonably expect that their communication is private and confidential (see, for example, *Altay v. Turkey* (no. 2), no. 11236/06, §§ 49-51, 9 April 2019, and the references therein). […]

55. Firstly, the Court takes note of the circumstance that the proceedings relating to the filtering

of LPP in cases such as the present one lacked a clear basis in the Code of Criminal Procedure right from the outset, which rendered them liable to disputes such as that which followed the Supreme Court's decision of 16 January 2017. Secondly, the actual form of the proceedings could hardly be foreseeable to the applicant – notwithstanding that he was allowed to object (see paragraph 12 above) – given that they were effectively reorganised following that decision. Thirdly, and most importantly, the Court finds that the Government have not rebutted the applicant's contention that subsequently to the Supreme Court's finding in its decision of 16 January 2017 that the police should themselves examine the data carriers in cases such as the present one, the decision to apply that instruction to the applicant's ongoing case, which became final with the Supreme Court's decision of 30 June 2017 (see paragraph 26 above), meant that no clear and specific procedural guarantees were in place to prevent LPP from being compromised by the search of the mirror image copy of his phone. The Supreme Court had not given any instructions as to how the police were to carry out the task of filtering LPP, apart from indicating that search words should be decided upon in consultation with counsel; even though the claim lodged for LPP in the instant case was as such undisputedly valid, the mirror image copy was effectively just returned to the police for examination without any practical procedural scheme in place for that purpose. As to the report of 9 November 2017 (see paragraph 27 above), it described the deletion of data in the applicant's case, but did not describe any clear basis or form for the procedure either.

56. In this context the Court emphasises that it has noted that the Government did indeed point to the procedural safeguards in place relating to searches and seizures in general; the Court's concern is, however, the lack of an established framework for the protection of LPP in cases such as the present one. […]

57. Although no such regulation was in place in the applicant's case, the Court has no basis to decide whether or not LPP was actually compromised in his case, nor has the applicant submitted that it was. In the Court's view, however, the lack of foreseeability in the instant case, due to the lack of clarity in the legal framework and the lack of procedural guarantees relating concretely to the protection of LPP, already fell short of the requirements flowing from the criterion that the interference must be in accordance with the law within the meaning of Article 8 § 2 of the Convention. Having drawn that conclusion, it is not necessary for the Court to review compliance with the other requirements under that provision.

***Kopp v Switzerland*, App No 23224/94, Judgment, European Court of Human Rights (25 March 1998)**

71. […] [The Government] added that Mr Kopp, the husband of a former member of the Federal Council, had not had his telephones tapped in his capacity as a lawyer. In the instant case, in accordance with Swiss telephone-monitoring practice, a specialist Post Office official had listened to the tape in order to identify any conversations relevant to the proceedings in progress, but no recording had been put aside and sent to the Federal Public Prosecutor's Office.

72. The Court, however, is not persuaded by these arguments. Firstly, it is not for the Court to speculate as to the capacity in which Mr Kopp had had his telephones tapped, since he was a lawyer and all his law firm's telephone lines had been monitored. Secondly, tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated. In that connection, the Court by no means seeks to minimise the value of some of the safeguards built into the law, such as the requirement at the relevant stage of the proceedings that the prosecuting authorities' telephone-tapping order must be approved by the President of the Indictment Division, who is an independent judge, or the fact that the applicant was officially informed that his telephone calls had been intercepted.

73. However, the Court discerns a contradiction between the clear text of legislation which protects legal professional privilege when a lawyer is being monitored as a third party and the practice followed in the present case. Even though the case-law has established the principle, which is moreover generally accepted, that legal professional privilege covers only the relationship between a lawyer and his clients, the law does not clearly state how, under what conditions and by whom the distinction is to be drawn between matters specifically connected with a lawyer's work under instructions from a party to proceedings and those relating to activity other than that of counsel.

74. Above all, in practice, it is, to say the least, astonishing that this task should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of the defence.

75. In short, Swiss law, whether written or unwritten, does not indicate with sufficient clarity the scope and manner of exercise of the authorities' discretion in the matter. Consequently, Mr Kopp, as a lawyer, did not enjoy the minimum degree of protection required by the rule of law in a democratic society. There has therefore been a breach of Article 8.

Annual Report of the Inter-American Commission on Human Rights 2020, Volume II – Annual Report of the Office of the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II Doc 28 (30 March 2021)

174. States should take the necessary measures to ensure that confidential sources and materials related to the disclosure of restricted information are protected by law. In the digital era, the right to the confidentiality of sources may entail a set of additional positive obligations aimed at ensuring the privacy of communications and preventing state surveillance actions from being disproportionate and directly or indirectly violating or jeopardizing these rights.

***Särgava v Estonia*, App No 698/19, Judgment, European Court of Human Rights (16 November 2021)**

69. […] The Court reiterates that it is incumbent on the Government pleading non-exhaustion to satisfy it that the remedy was an effective one available in theory and in practice at the relevant time, that is to say that it was accessible, was capable of providing redress in respect of the applicant's complaints and offered reasonable prospects of success (see *Molla Sali v. Greece* (just satisfaction) [GC], no. 20452/14, § 89, 18 June 2020). In the case at hand, the Government have not explained what the practical consequences of the applicant's possible request under Article 225 of the CCrP could be. Nor has the Government presented any examples of the practical application of this alleged remedy, not least in the context of challenging the seizure of data carriers allegedly containing material covered by lawyer-client confidentiality. The Court has doubts as to whether in such circumstances the review by the prosecutor's office would meet the requisite standards of independence (compare *Avanesyan v. Russia*, no. 41152/06, § 32, 18 September 2014, and *Panteleyenko v. Ukraine*, no. 11901/02, § 80, 29 June 2006), and it is not clear whether a possible refusal by the prosecutor's office would be subject to a judicial review. In any event, the Court observes that by the time the applicant could have made use of that alleged remedy, the keyword-based examination of the copied content of his mobile telephone and laptop had already been carried out (see paragraphs **Error! Reference source not found.-Error! Reference source not found.** above).

85. In so far as the applicant complains about the seizure of his data carriers and their subsequent examination, the Court finds that those acts constituted an interference with his right to respect for

his "correspondence". The failure of the applicant or his lawyer to invoke legal professional privilege immediately during the search (see the Government's argument in paragraph **Error! Reference source not found.** above) does not alter that finding. […]

86. As to the question of whether the measure was in accordance with the law, the Court's case-law has established that a measure must have some basis in domestic law, the term "law" being understood in its "substantive" rather than its "formal" sense. In a sphere covered by statutory law, the "law" is the enactment in force as the competent courts have interpreted it. Domestic law must further be compatible with the rule of law and accessible to the person concerned, and the person affected must be able to foresee the consequences of the domestic law for him or her (see *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13 and 2 others, § 332, 25 May 2021; *Wolland v. Norway*, no. 39731/12, § 62, 17 May 2018; see also *Golovan v. Ukraine*, no. 41716/06, § 56, 5 July 2012).

87. In the context of searches and seizures, the domestic law must provide some protection to the individual against arbitrary interference with Article 8 rights. It must thus be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances and conditions under which public authorities are empowered to resort to any such measures (see *Golovan*, cited above, § 57).

88. Furthermore, the Court has acknowledged the importance of specific procedural guarantees when it comes to protecting the confidentiality of exchanges between lawyers and their clients (see *Saber v. Norway,* no. 459/18, § 51, 17 December 2020, and *Sommer v. Germany*, no. 73607/13, § 56, 27 April 2017; see also *Kadura and Smaliy v. Ukraine*, nos. 42753/14 and 43860/14, §§ 144-45, 21 January 2021).

89. The Convention does not prohibit the imposition on lawyers of certain obligations likely to concern their relationships with their clients. This is the case in particular where credible evidence is found of the participation of a lawyer in an offence, or in connection with efforts to combat certain practices. On that account, however, it is vital to provide a strict framework for such measures, since lawyers occupy a vital position in the administration of justice and can, by virtue of their role as intermediary between litigants and the courts, be described as officers of the law (see *André and Another v. France*, no. 18603/03, § 42, 24 July 2008).

98. Despite the safeguards referred to above, the Court's essential concern is the lack of a practical framework for the protection of legal professional privilege in cases such as the present one. Working on the premise that under domestic law professional legal privilege does not apply to the extent that the lawyer him or herself is a suspect and/or acted in a capacity other than a lawyer, the key question is how privileged material is distinguished and separated from material where the lawyer-client confidentiality cannot be relied on. The Court notes that it was not established in the domestic proceedings and that it clearly does not follow from the Government's observations that under domestic law lawyer-client confidentiality stops applying altogether with respect to a lawyer who is a suspect in a criminal case, or who also engages in activities other than providing legal services and/or fails to duly separate various privileged and non-privileged material.

99. While the question of sifting and separating privileged and non-privileged files is undoubtedly important in the context of hard copy material, it becomes even more relevant in a situation where the privileged content is part of larger batches of digitally stored data. In such a situation, even if the lawyer concerned or his representative is present at the search site, it might prove difficult to distinguish swiftly during the search which exact electronic files are covered by legal professional privilege and which are not.

100. The question of how to carry out sufficiently targeted sifting is equally pertinent in circumstances where under domestic law or practice such sifting is not carried out at the site of the search, but the data carriers are instead seized in their entirety and/or a mirror-image copy of their content is made. In that regard, the Court is prepared to accept the Government's argument that making a mirror-

image copy can been seen as a procedural guarantee against any possible manipulation of the content of those data carriers (see *Wolland*, cited above, § 76; compare and contrast *Iliya Stefanov v. Bulgaria*, no. 65755/01, § 42, 22 May 2008, and *Kolesnichenko v. Russia*, no. 19856/04, § 43, 9 April 2009). Such a practice would, moreover, allow the authorities to return the seized data carriers relatively promptly to their owners and – should the owners be lawyers or law firms – avoid their work from being unduly inhibited for longer than is absolutely necessary.

102. The Court draws attention to the fact that in addition to safeguards addressing the seizure of data carriers and/or copying of their content as well as the sifting of digitally stored data, it is also important to prevent unwarranted and unrecorded access to the data carriers and/or processing of the data from the moment that it is seized until it is either returned or destroyed in due course.

103. Turning to the circumstances of the instant case, the Court observes that the domestic law does not seem to contain any specific procedure or safeguards to address the examination of electronic data carriers and prevent communication covered by legal professional privilege from being compromised. The Court considers that this lack of a practical procedural scheme and safeguards is, to a lesser or greater extent, also reflected in how, in the instant case, the search was authorised and how the subsequent copying of the seized data carriers and the examination of their content was carried out.

104. In the case of the applicant, the search warrant issued by the preliminary investigation judge made no provision for safeguarding the possible privileged material protected by professional secrecy (compare *Kruglov and Others v. Russia*, nos. 11264/04 and 15 others, §§ 128-29, 4 February 2020; *Iliya Stefanov*, cited above, § 41; and *Smirnov v. Russia*, no. 71362/01, § 46, 7 June 2007). This was the situation despite the fact that the State Prosecutor's application for a search warrant had specifically included reference to the possibility that the applicant might be in possession of information related to his professional activities as a lawyer but that would not be of relevance in the context of the ongoing criminal proceedings (see paragraph **Error! Reference source not found.** above).

105. Although the applicant was later assured that the search of the content of his laptop and mobile telephone would take place on the basis of keywords – and such a search was indeed carried out – this obligation did not seem to derive from domestic legislation. Accordingly, the keyword-based search was not envisaged in the State Prosecutor's application for authorisation of a search, nor was such an obligation mentioned by the preliminary investigation judge in the search warrants (compare *Sérvulo & Associados - Sociedade de Advogados, RL and Others v. Portugal*, no. 27013/10, 3 September 2015).

106. Rather, it appears that the decision of whether to conduct a keyword-based search (or use any other method of sifting) as well as the choice of relevant keywords was left entirely up to the investigative authorities. At this juncture, the Court observes that some of the keywords used for the search (such as "financial year" or "credit line") were notably broad in scope. The Court has already found above that the domestic law did not grant the applicant any right to be present during the keyword-based search (see paragraph **Error! Reference source not found.** above).

107. In any event, it remains unclear from the domestic law how any potential disputes between the investigative authorities and the lawyer concerned over the keywords to be used or any other methods of filtering the electronic content would be resolved. Indeed, the domestic law does not seem to have any specific rules about the procedure to be followed in the event that either the lawyer or his representative objects to the seizure or content examination with reference to lawyer-client confidentiality (compare, for example, *Robathin v. Austria*, no. 30457/06, § 50, 3 July 2012; *Wieser and Bicos Beteiligungen GmbH v. Austria*, no. 74336/01, §§ 60 and 62, ECHR 2007-IV; and *André and Another*, cited above, § 44). The Court notes that the domestic law provides for the possibility to lodge an appeal against investigative activities. However, it does not appear to follow from the domestic law that material in respect of which the applicability of legal professional privilege is

disputed would not be made available to the investigative authorities before the domestic courts have had a chance to conduct a specific and detailed analysis of the matter, and – if necessary – order the return or destruction of seized data carriers and/or their copied content (compare *Kırdök and Others v. Turkey*, no. 14704/12, § 51, 3 December 2019; *Vinci Construction and GTM Génie Civil et Services v. France*, nos. 63629/10 and 60567/10, § 79, 2 April 2015).

109. Although the domestic legislation lacked the appropriate procedural safeguards in order to protect data covered by legal professional privilege, the Court has no basis on which to decide whether or not lawyer-client confidentiality was actually compromised in the case at hand. In the Court's view, however, the lack of procedural guarantees relating specifically to the protection of legal professional privilege already fell short of the requirements flowing from the criterion that the interference must be in accordance with the law within the meaning of Article 8 § 2 of the Convention (see *Saber*, cited above, § 57). Having drawn that conclusion, it is not necessary for the Court to review compliance with the other requirements under that provision.

Vasil Vasilev v Bulgaria, App No 7610/15, Judgment, European Court of Human Rights (16 November 2021)

89. […] Moreover, specific procedural guarantees are needed when it comes to protecting the confidentiality of lawyer-client communications (see Saber v. Norway, no. 459/18, § 51, 17 December 2020). This is because Article 8 of the Convention, although safeguarding the confidentiality of any "correspondence", affords strengthened protection to exchanges between lawyers and their clients (see Michaud v. France, no. 12323/11, § 118, ECHR 2012; R.E. v. the United Kingdom, no. 62498/11, § 131, 27 October 2015; and Dudchenko, cited above, § 104).

93. It is open to question, however, whether the instruction, which was a purely internal act issued pursuant to the Chief Prosecutor's power to make instructions governing the work of the prosecuting authorities, can be seen as "law" for the purposes of Article 8 § 2 of the Convention (see, mutatis mutandis, Silver and Others v. the United Kingdom, 25 March 1983, § 86, Series A no. 61; Malone, cited above, §§ 68 and 79; and Amann, cited above, § 75). It is moreover doubtful whether that instruction lays down enough safeguards to protect accidentally intercepted lawyer-client communications (see, mutatis mutandis, R.E. v. the United Kingdom, §§ 138-41, and Dudchenko, § 107, both cited above). Its only provision dealing with the point simply says that that if the authorities intercept the conversation of a lawyer with a client or with another lawyer, and that conversation touches upon a client's defence, they must not prepare evidentiary materials on its basis, unless the surveillance reveals that the lawyer has him- or herself engaged in criminal activity (see paragraph 39 above). That leaves open the question how precisely any such intercept materials are to be handled and destroyed, as required under section 33(3) of the Bar Act 2004. Nor does the instruction seem to encompass all sorts of lawyer-client communications; by its terms, it appears to cover solely communications relating to a client's defence – which implies already pending litigation, and perhaps even just criminal proceedings. Lastly and perhaps most importantly for the purposes of the present case, the instruction was issued more than a year after the covert interception of the applicant's conversation, and recognised in its preamble that the matter had hitherto been subject to inconsistent practices (see paragraph 37 above, and compare with R.E. v. the United Kingdom, cited above, § 140 in fine).

***Kadura and Smaliy v Ukraine,* Apps Nos 42753/14 and 43860/14, Judgment, European Court of Human Rights (21 January 2021)**

142. An encroachment on professional secrecy of lawyers may have repercussions for the proper administration of justice and hence for the rights guaranteed by Article 6 of the Convention. The authorities must have a compelling reason for interfering with the secrecy of a lawyer's communications or with his working papers.

144. In performing the search and the seizure of the documents and the telephone incidental to the

arrest the authorities gave no consideration to the special status of the seized material as possibly containing privileged information. No reason was cited at any point for the decision to conduct the seizure and there was no indication that there were any safeguards in place to ensure proper handling of the information potentially subject to the lawyer's professional privilege.

146. Accordingly, it has not been shown that there were any safeguards in place against the authorities accessing, improperly and arbitrarily, information subject to legal professional privilege. The domestic investigation in that respect is still pending and was, therefore, unable to dispel the difficulties at the heart of the applicant's Article 8 complaint. On the basis of the information available to it the Court must conclude that it has not been shown that the interference with the applicant's rights was "in accordance with the law".

147. There has, accordingly, been a violation of Article 8 of the Convention in respect of Mr Smaliy on account of his search and the seizure of his telephone and documents.

***Kruglov and Others v Russia*, Apps Nos 11264/04 and 15 others, Judgment, European Court of Human Rights (4 February 2020)**

125. […] To determine whether the measures were "necessary in a democratic society", the Court has to ascertain whether effective safeguards against abuse or arbitrariness were available under domestic law and how those safeguards operated in the specific cases under examination. Elements to be taken into consideration in this regard are the severity of the offence in connection with which the search and seizure were effected, whether they were carried out pursuant to an order issued by a judge or a judicial officer or subjected to after-the-fact judicial scrutiny, whether the order was based on reasonable suspicion, and whether its scope was reasonably limited. The Court must also review the manner in which the search was executed, including – where a lawyer's office is concerned – whether it was carried out in the presence of an independent observer or whether other special safeguards were available to ensure that material covered by legal professional privilege was not removed. The Court must lastly take into account the extent of the possible repercussions on the work and the reputation of the persons affected by the search (see *Yuditskaya*, cited above, § 27).

127. […] According to the Court's case-law, search warrants have to be drafted, as far as practicable, in a manner calculated to keep their impact within reasonable bounds.

128. […] On the contrary, in issuing the search warrants, the courts seemed to imply that lawyer-client confidentiality could be breached in every case as long as there was a criminal investigation, even where such investigation was not against the lawyers but against their clients.

129. The Court concludes that in the cases where a court search warrant was issued, the national courts did not carry out a balancing exercise or examine whether the interference with the applicants' rights had answered a pressing social need and was proportionate to the legitimate aims pursued.

136. Having regard to the above, the Court finds that the searches in the present cases impinged on professional confidentiality to an extent that was disproportionate to the legitimate aim being pursued.

***Dudchenko v Russia*, App No 37717/05, Judgment, European Court of Human Rights (7 November 2017)**

104. The Court reiterates that, while Article 8 protects the confidentiality of all correspondence between individuals, it will afford "strengthened protection" to exchanges between lawyers and their clients, as lawyers would be unable to defend their clients if they were unable to guarantee that their exchanges would remain confidential.

105. In its case-law the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power in cases where legally privileged material has been acquired through measures of secret surveillance.

106. Firstly, the law must clearly define the scope of the legal professional privilege and state how, under what conditions and by whom the distinction is to be drawn between privileged and non-privileged material. Given that the confidential relations between a lawyer and his clients belong to an especially sensitive area which directly concern the rights of the defence, it is unacceptable that this task should be assigned to a member of the executive, without supervision by an independent judge.

107. Secondly, the legal provisions concerning the examination, use and storage of the material obtained, the precautions to be taken when communicating the material to other parties, and the circumstances in which recordings may or must be erased or the material destroyed must provide sufficient safeguards for the protection of the legally privileged material obtained by covert surveillance. In particular, the national law should set out with sufficient clarity and detail: procedures for reporting to an independent supervisory authority for review of cases where material subject to legal professional privilege has been acquired as a result of secret surveillance; procedures for secure destruction of such material; conditions under which it may be retained and used in criminal proceedings and law-enforcement investigations; and, in that case, procedures for safe storage, dissemination of such material and its subsequent destruction as soon as it is no longer required for any of the authorised purposes. […]

109. Most importantly for the case at hand, the domestic law does not provide for any safeguards to be applied or any procedures to be followed in cases where, while tapping a suspect's telephone, the authorities accidentally intercept the suspect's conversations with his or her counsel.

110. It follows that Russian law does not provide for any safeguards against abuse of power in cases where legally privileged material has been acquired through measures of secret surveillance and does not therefore meet the "quality of law" requirement. It also follows that the surveillance measures applied to the applicant did not meet the requirements of Article 8 § 2 of the Convention as elucidated in the Court's case-law.

***Sommer v Germany*, App No 73607/13, Judgment, European Court of Human Rights (27 April 2017)**

48. […] the Court agrees with the parties and holds that collecting, storing and making available the applicant's professional bank transactions constituted an interference with his right to respect for professional confidentiality and his private life. […]

52. As regards the protection of the professional confidentiality of lawyers, the Court observes that Article 160a § 4 of the [Code of Criminal Procedure (CCP)] does not require there to be a formal investigation against the lawyer who is affected, but that the prohibition of investigative measures against lawyers under Article 160a §§ (1) to (3) of the CCP can be lifted if certain facts substantiate a suspicion of participation in an offence.

53. […] It reiterates that, in the context of covert intelligence-gathering, it is essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness. […]

56. […], the Court has previously acknowledged the importance of specific procedural guarantees when it comes to protecting the confidentiality of exchanges between lawyer and client and of legal professional privilege. It has emphasised that, subject to strict supervision, it is possible to impose

certain obligations on lawyers concerning their relations with their clients, for example in the event that there is plausible evidence of the lawyer's involvement in a crime and in the context of the fight against money-laundering. The Court has further elaborated that the Convention does not prevent domestic law allowing for searches of a lawyer's offices as long as proper safeguards are provided, for example the presence of a representative (or president) of a bar association.

57. Turning to the facts of the present case, the Court firstly notes the wide scope of the prosecutorial requests for information, which concerned information about all transactions relating to the applicant's professional bank account for a period of over two years, as well as information about further, possibly private, bank accounts of the applicant. It agrees with the applicant that the information submitted by the bank provided the public prosecutor and the police with a complete picture of his professional activity for the time in question, and moreover with information about his clients...The fact that only fifty-three transactions were considered relevant and included in the case file, and that the Regional Court restricted access to the relevant parts of the case file later on, could not redress the already ongoing interference, but only limit it from becoming more serious. In sum, the Court concludes that the requests for information were only limited in relation to the period in question, but otherwise concerned all information concerning the bank account and banking transactions of the applicant. […]

61. The Court observes that Article 160a of the CCP provides a specific safeguard for lawyers and lawyer-client privilege. However, it also notes that such protection can be suspended under Article 160a § 4 of the CCP if certain facts substantiate a suspicion of participation in an offence. According to the Government, with reference to the discussions during the legislative procedure, Article 160a § 4 of the CCP does not require there to be an official investigation against a lawyer before the protection of the professional confidentiality of lawyers is suspended. According to the national authorities and courts, the transfer of fees from the applicant's client's fiancée to the applicant, and the suspicion that money stemming from illegal activities had been transferred to the fiancée's bank account, sufficiently substantiated a suspicion against the applicant. On the basis of the information and documents provided by the parties, the Court considers that the suspicion against the applicant was rather vague and unspecific.

62. Lastly, the Court observes that the inspection of the applicant's bank account was not ordered by a judicial authority, and that no "specific procedural guarantees" were applied to protect legal professional privilege. In so far as the Government submitted that the applicant could have the measures reviewed by a court under the analogous application of Article 98 § 2 of the CCP, the Court reiterates that a subsequent judicial review can offer sufficient protection if a review procedure at an earlier stage would jeopardise the purpose of an investigation or surveillance. However, the effectiveness of a subsequent judicial review is inextricably linked to the question of subsequent notification about the surveillance measures. There is, in principle, little scope for recourse to the courts by an individual unless he or she is advised of the measures taken without his or her knowledge and thus able to challenge the legality of such measures retrospectively. In that regard, the Court observes that the public prosecutor asked the bank not to reveal his information requests to the applicant, that the applicant was not informed about the inspection of his professional bank account by the public prosecutor, and that he only learned of the investigative measures concerning his own bank account from the case file. The Court concludes that, even though there was no legal requirement to notify the applicant, by coincidence he learnt of the investigative measures and had access to a retrospective judicial review of the prosecutorial requests for information.

63. Having regard to the low threshold for inspecting the applicant's bank account, the wide scope of the requests for information, the subsequent disclosure and continuing storage of the applicant's personal information, and the insufficiency of procedural safeguards, the Court concludes that the interference was not proportionate and therefore not "necessary in a democratic society". […]

***Iordachi and Others v Moldova*, App No 25198/02, Judgment, European Court of Human Rights (10 February 2009)**

50. As regards the interception of communications of persons suspected of offences, the Court observes that in Kopp it found a violation of Article 8 because the person empowered under Swiss secret surveillance law to draw a distinction between matters connected with a lawyer's work and other matters was an official of the Post Office's legal department. In the present case, while the Moldovan legislation, like the Swiss legislation, guarantees the secrecy of lawyer-client communications, it does not provide for any procedure which would give substance to the above provision. The Court is struck by the absence of clear rules defining what should happen when, for example, a phone call made by a client to his lawyer is intercepted.

***Tristán Donoso v Panamá*, Inter-American Court of Human Rights, Judgment (on Preliminary Objection, Merits, Reparations, and Costs) Series C No 193 (27 January 2009)**

75. The Court considers the telephone conversation between Mr. Zayed and Mr. Tristán Donoso to have been private and that none of the two of them consented to its disclosure to third parties. Moreover, as such conversation was held between the alleged victim [A Lawyer] and one of his clients, it should even be afforded a greater degree of protection on account of professional secrecy.'

B. PROFESSIONAL CONFIDENTIALITY AND PRIVILEGED COMMUNICATIONS – PROTECTION OF JOURNALISTS' SOURCES

***Big Brother Watch and Others v The United Kingdom*, Apps Nos 58170/13, 62322/14 and 24960/15, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

(a) General principles on the protection of journalists' sources

442. As freedom of expression constitutes one of the essential foundations of a democratic society, the Court has always subjected the safeguards for respect of freedom of expression in cases under Article 10 of the Convention to special scrutiny. The safeguards to be afforded to the press are of particular importance, and the protection of journalistic sources is one of the cornerstones of freedom of the press. Without such protection, sources may be deterred from assisting the press in informing the public about matters of public interest. As a result the vital public-watchdog role of the press may be undermined, and the ability of the press to provide accurate and reliable information may be affected adversely (see, inter alia, *Goodwin v. the United Kingdom*, no. 17488/90, § 39, 27 March 1996; *Sanoma Uitgevers B.V.*, cited above, § 50; and *Weber and Saravia*, cited above, § 143).

443. Orders to disclose sources potentially have a detrimental impact, not only on the source, whose identity may be revealed, but also on the newspaper or other publication against which the order is directed, whose reputation may be negatively affected in the eyes of future potential sources by the disclosure; and on members of the public, who have an interest in receiving information imparted through anonymous sources. There is, however, "a fundamental difference" between the authorities ordering a journalist to reveal the identity of his or her sources, and the authorities carrying out searches at a journalist's home and workplace with a view to uncovering his or her sources (compare *Goodwin*, cited above, § 39, with *Roemen and Schmit v. Luxembourg*, no. 51772/99, § 57, ECHR 2003-IV). The latter, even if unproductive, constitutes a more drastic measure than an order to divulge a source's identity, since investigators who raid a journalist's workplace have access to all the documentation held by the journalist (see *Roemen and Schmit*, cited above, § 57).

444. An interference with the protection of journalistic sources cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest (see

Sanoma Uitgevers B.V., cited above, § 51; Goodwin, cited above, § 39; *Roemen and Schmit*, cited above, § 46; and *Voskuil v. the Netherlands*, no. 64752/01, § 65, 22 November 2007). Furthermore, any interference with the right to protection of journalistic sources must be attended with legal procedural safeguards commensurate with the importance of the principle at stake (see *Sanoma Uitgevers B.V.*, cited above, §§ 88-89). First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making body with the power to determine whether a requirement in the public interest overriding the principle of protection of journalistic sources exists prior to the handing over of such material and to prevent unnecessary access to information capable of disclosing the sources' identity if it does not (see *Sanoma Uitgevers B.V.*, cited above, §§ 88-90).

445. Given the preventive nature of such review the judge or other independent and impartial body must be in a position to carry out this weighing of the potential risks and respective interests prior to any disclosure and with reference to the material that it is sought to have disclosed so that the arguments of the authorities seeking the disclosure can be assessed properly. The decision to be taken should be governed by clear criteria, including whether a less intrusive measure can suffice to serve the overriding public interests established. It should be open to the judge or other authority to refuse to make a disclosure order or to make a limited or qualified order so as to protect sources from being revealed, whether or not they are specifically named in the withheld material, on the grounds that the communication of such material creates a serious risk of compromising the identity of journalist's sources (see *Sanoma Uitgevers B.V.*, cited above, § 92 and *Nordisk Film & TV A/S v. Denmark* (dec.), no. 40485/02, ECHR 2005-XIII). In situations of urgency, a procedure should exist to identify and isolate, prior to the exploitation of the material by the authorities, information that could lead to the identification of sources from information that carries no such risk (see, mutatis mutandis, *Wieser and Bicos Beteiligungen GmbH v. Austria*, no. 74336/01, §§ 62-66, ECHR 2007-XI).

(b) Article 10 in the bulk interception context
446. In Weber and Saravia the Court recognised that the "strategic monitoring" regime had interfered with the first applicant's freedom of expression as a journalist. However, in so finding it considered it decisive that the surveillance measures were not aimed at monitoring journalists or uncovering journalistic sources. As such, it found that the interference with the first applicant's freedom of expression could not be characterised as particularly serious and, in view of the attendant safeguards, it declared her complaints inadmissible as manifestly ill-founded (see *Weber and Saravia*, cited above, §§ 143-145 and 151).

(c) The approach to be adopted in the present case
447. Under the section 8(4) regime, confidential journalistic material could have been accessed by the intelligence services either intentionally, through the deliberate use of selectors or search terms connected to a journalist or news organisation, or unintentionally, as a "bycatch" of the bulk interception operation.

448. Where the intention of the intelligence services is to access confidential journalistic material, for example, through the deliberate use of a strong selector connected to a journalist, or where, as a result of the choice of such strong selectors, there is a high probability that such material will be selected for examination, the Court considers that the interference will be commensurate with that occasioned by the search of a journalist's home or workplace; regardless of whether or not the intelligence services' intention is to identify a source, the use of selectors or search terms connected to a journalist would very likely result in the acquisition of significant amounts of confidential journalistic material which could undermine the protection of sources to an even greater extent than an order to disclose a source (see *Roemen and Schmit*, cited above, § 57). Therefore, the Court considers that before the intelligence services use selectors or search terms known to be connected to a journalist, or which would make the selection of confidential journalistic material for examination highly probable, the selectors or search terms must have

been authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether they were "justified by an overriding requirement in the public interest" and, in particular, whether a less intrusive measure might have sufficed to serve the overriding public interest (see *Sanoma Uitgevers B.V.*, cited above, §§ 90-92).

449. Even where there is no intention to access confidential journalistic material, and the selectors and search terms used are not such as to make the selection of confidential journalistic material for examination highly probable, there will nevertheless be a risk that such material could be intercepted, and even examined, as a "bycatch" of a bulk interception operation. In the Court's view, this situation is materially different from the targeted surveillance of a journalist through either the section 8(1) or the section 8(4) regimes. As the interception of any journalistic communications would be inadvertent, the degree of interference with journalistic communications and/or sources could not be predicted at the outset. Consequently, it would not be possible at the authorisation stage for a judge or other independent body to assess whether any such interference would be "justified by an overriding requirement in the public interest" and, in particular, whether a less intrusive measure might have sufficed to serve the overriding public interest.

450. In *Weber and Saravia* the Court held that the interference with freedom of expression caused by strategic monitoring could not be characterised as particularly serious as it was not aimed at monitoring journalists and the authorities would know only when examining the intercepted telecommunications, if at all, that a journalist's communications had been monitored (see Weber and Saravia, cited above, § 151). Therefore, it accepted that the initial interception, without examination of the intercepted material, did not constitute a serious interference with Article 10 of the Convention. Nevertheless, as the Court has already observed, in the current, increasingly digital, age technological capabilities have greatly increased the volume of communications traversing the global Internet, and as a consequence surveillance which is not targeted directly at individuals has the capacity to have a very wide reach indeed, both within and without the territory of the surveilling State (see paragraphs 322-323 above). As the examination of a journalist's communications or related communications data by an analyst would be capable of leading to the identification of a source, the Court considers it imperative that domestic law contain robust safeguards regarding the storage, examination, use, onward transmission and destruction of such confidential material. Moreover, even if a journalistic communication or related communications data have not been selected for examination through the deliberate use of a selector or search term known to be connected to a journalist, if and when it becomes apparent that the communication or related communications data contain confidential journalistic material, their continued storage and examination by an analyst should only be possible if authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether continued storage and examination is "justified by an overriding requirement in the public interest".

***Svetova and Others v Russia*, App No 54714/17, Judgment, European Court of Human Rights (24 January 2023)**

40. The Court further notes that the search warrant was issued fourteen years after the opening of a criminal case against the third parties and was executed forty days after it had been issued. Such a wide time frame, in the absence of any explanation, makes doubtful its usefulness for the investigation.

44. Next, the Court notes that, even if the purpose of the searches and seizures was not to uncover Ms Svetova's journalistic sources, the vagueness of the formulations and the unrestricted discretion in the determination of the scope of the search were too broad to rule out that possibility. They, therefore, constituted an interference with Ms Svetova's journalistic freedom of expression and were

disproportionate and not "necessary in a democratic society" within the meaning of Article 10 § 2 (see *Avaz Zeynalov*, cited above, § 104, and *Sergey Sorokin v. Russia*, 52808/09, §§ 62-64, 30 August 2022, with further references).

***Sedletska v Ukraine*, App No 42634/18, Judgment, European Court of Human Rights (1 April 2021)**

62. […] An interference potentially leading to disclosure of a source cannot be considered "necessary" under Article 10 § 2 unless it is justified by an overriding requirement in the public interest […]. The Court has previously held that to establish the existence of an "overriding requirement" it may not be sufficient for a party seeking disclosure of a source to show merely that he or she will be unable without disclosure to exercise the legal right or avert the threatened legal wrong on which he or she bases the claim: the considerations to be taken into account by the Court for its review under Article 10 § 2 tip the balance of competing interests in favour of the interest of democratic society in securing a free press.

65. In this connection, the Court notes firstly that the District Court's order of 27 August 2018 authorised the PGO to collect a wide range of the applicant's protected communications data concerning her personal and professional contacts over a sixteen-month period. The disputed authorisation included, in particular, access to information concerning the time and duration of the applicant's communications and the telephone numbers of her contacts […]. This data could possibly include identifiable information concerning the applicant's confidential sources which had no relevance to the criminal proceedings regarding the alleged misconduct of S. The risk of detriment to the interests protected by Article 10 was all the greater as the focus of the applicant's work as a journalist had been on investigating high-profile corruption, including corruption within the PGO itself. The District Court's order contained no safeguards excluding the possibility that information potentially leading to the identification of any such sources would become available to a wide circle of PGO officials and could be used for purposes unrelated to the criminal investigation concerning S. These elements are sufficient for the Court to conclude that the scope of the data access authorisation in the court order of 27 August 2018 was grossly disproportionate to the legitimate aims of investigating a purported leak of classified information by S. and protecting Ms N.'s private life. […]

71. The Court finds that the text of the Court of Appeal's ruling did not sufficiently respond to these requirements. Firstly, this ruling authorised access to the applicant's protected geolocation data over a sixteen-month period. In view of the length of that period and the size of the geographical area of the city centre of Kyiv in respect of which the geolocation data was sought, the applicant's telephone could have been registered there on a number of occasions which had no relevance to the case under investigation by the PGO. Secondly, by way of justifying the pressing social need for the interference with the applicant's rights, the Court of Appeal referred only to the purpose of "achieving efficiency" in a criminal investigation and establishing "more exactly the time and place" of the purported confidential meeting (see paragraph 22 above) without providing any indication why these considerations outweighed the public interest in non-disclosure of the applicant's protected geolocation data. Thirdly, based on the case file, at the relevant time there remained considerable uncertainty that any information pertinent to the proceedings against S. would be retrieved from the applicant's communications data. It appears from the material in the Court's possession that at the relevant time it had not been unequivocally established that S.'s alleged meeting with the journalists had been held on the NABU's premises or some other premises located within the geographical area targeted by the PGO for the collection of the applicant's geolocation data, or that the applicant had indeed been a participant in the meeting. Even so, the applicant might not have necessarily had her telephone with her at the time. Fourthly, it does not appear that the Court of Appeal delved into the question whether there were other more targeted means of obtaining the information which the investigative authority had hoped to retrieve from the applicant's communications data.

72. In view of the above considerations, the Court is not convinced that the data access authorisation

given by the domestic courts was justified by an "overriding requirement in the public interest" and, therefore, necessary in a democratic society (see *Goodwin*, cited above, § 45; *Voskuil*, cited above, § 72; and *Becker*, cited above, § 83).

Annual Report of the Inter-American Commission on Human Rights 2019, Volume II – Annual Report of the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II. Doc 5 (24 February 2020)

24. Regarding the reservation of journalistic sources, this Office received information on cases in Argentina and Brazil, arguing that investigative journalism would be in danger as a result of some measures carried out by judicial authorities, which would seek to identify the sources of journalistic material that would have served as the basis for uncovering alleged corruption plots. Likewise, there would have been violations to source confidentiality in Canada and the United States.

25. In relation to this point, as in previous years, the Office of the Special Rapporteur recommends Member States to: C. Abstain from punishing journalists, members of the media or members of civil society who have access to and disseminate reserved information about this type of surveillance programs, considering it to be of public interest. Confidential sources and materials associated with dissemination of reserved information must be protected by law.

C. SAFETY OF JOURNALISTS AND HUMAN RIGHTS DEFENDERS

The review of pronouncements by different human rights monitoring mechanisms shows that there are significant overlaps in references to encryption, the protection of journalists and human rights defenders. For this reason, it may be helpful to consult the content of all the relevant sub-chapters.

UN General Assembly Resolution on the Safety of journalists and the issue of impunity, UN Doc A/RES/78/215 (19 December 2023)*

Acknowledging the particular risks with regard to the safety of journalists in the digital age, including the particular vulnerability of journalists to becoming targets of unlawful or arbitrary surveillance or interception of communications, in violation of their rights to privacy and to freedom of expression,

18. *Emphasizes* that, in the digital age, encryption and anonymity tools have become vital for many journalists to freely exercise their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources, and calls upon States not to interfere with journalists' use of such technologies and to ensure that any restrictions thereon comply with States' obligations under international human rights law;

19. *Also emphasizes* the important role that media organizations can play in providing adequate safety, risk awareness, digital security and self-protection training and guidance to journalists and media workers, together with protective equipment;

** See also UN General Assembly Resolution on the Safety of Journalists and the Issue of Impunity, UN Doc A/RES/74/157 (18 December 2019); UN General Assembly Resolution on the Safety of Journalists and the Issue of Impunity, UN Doc A/RES/72/175 (19 December 2017); UN General Assembly Resolution on the Safety of Journalists and the Issue of Impunity, UN Doc A/RES/70/162 (17 December 2015)*

UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/51/9 (6 October 2022)*

Underlining that any measure or restriction introduced under emergency measures must be necessary, proportionate to the evaluated risk and applied in a non-discriminatory way, have a specific focus and duration, and be in accordance with the State's obligations under applicable international human rights law, and that the right to seek, receive and impart information requires that media freedom and the safety of journalists is protected during a state of emergency, including in the context of protests or during health crises,

Equally concerned about incidents of the extraterritorial targeting of journalists and media workers, including killings, enforced disappearances, harassment and surveillance,

Emphasizing the particular risks with regard to the safety of journalists in the digital age, including the particular vulnerability of journalists to becoming targets of unlawful or arbitrary surveillance and/or the interception of communications, hacking, including government-sponsored hacking, malware, spyware, forced data handover or denial of service attacks to force the shutdown of particular media websites or services, in violation of their rights to privacy and to freedom of expression,

11. *Calls upon* States:

(e) To ensure that measures to combat terrorism and preserve national security, public order or health are in compliance with their obligations under international law and do not arbitrarily or unduly hinder the work and safety of journalists, including through arbitrary arrest or detention, or the threat thereof;

(j) To protect in law and in practice the confidentiality of journalists' sources, including whistle-blowers, in acknowledgement of the essential role of journalists and those who provide them with information in fostering government accountability and an inclusive and peaceful society, subject only to limited and clearly defined exceptions provided for in national legal frameworks, including judicial authorization, in compliance with States' obligations under international human rights law;

(l) To refrain from interference with the use of technologies such as encryption and anonymity tools, and from employing unlawful or arbitrary surveillance techniques, including through hacking;

(m) To ensure that targeted surveillance technologies are only used in accordance with the human rights principles of lawfulness, legitimacy, necessity and proportionality, and that legal mechanisms of redress and effective remedies are available for victims of surveillance-related violations and abuses;

** See also UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/45/18 (12 October 2020); UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/39/6 (27 September 2018); UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/33/2 (29 September 2016)*

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

26. […] Targeted surveillance creates incentives for self-censorship and directly undermines the ability of journalists and human rights defenders to conduct investigations and build and maintain relationships with sources of information (A/HRC/38/35/Add.2, para. 53). […]

27. In addition to the primary obligations not to interfere with privacy or restrict expression, States also have duties to protect individuals against third-party interference. […] However, it is not clear that States generally afford affirmative legal protections against targeted surveillance. This is certainly true of transnational surveillance, even when committed by foreign entities against one's own citizens. […] [Human rights bodies] urged the Government [of Mexico] to allow an independent investigation of the allegations that the spyware was deployed against journalists (A/HRC/38/35/Add.2, paras. 52–55). To date, the efforts to investigate the allegations have not clarified the situation, despite the orders of the National Institute for Transparency, Access to Information and Personal Data Protection of Mexico that the Government reveal the nature of its contracts to obtain Pegasus.

48. Private companies are creating, transferring and servicing – and States are purchasing and using – surveillance technologies in troubling ways. Credible allegations have shown that companies are selling their tools to Governments that use them to target journalists, activists, opposition figures and others who play critical roles in democratic society. […]"

51. […] In this context, the law's default position should be to prohibit the use of digital surveillance tools against individuals in the media. Of course, this does not provide journalists with immunity from other forms of legitimate legal process, including non-digital surveillance. It is simply that, in the context of the intrusive technologies of digital surveillance, the possibility of abuse or "leakage" from a legitimate criminal investigation into areas involving other journalistic work is very real and difficult, if not impossible, to contain. Its very possibility would likely serve to deter journalists from working on the most sensitive sorts of topics, not to mention the willingness of sources and whistle-blowers to come forward.

Report of the Special Rapporteur on the Situation of Human Rights Defenders, Situation of Women Human Rights Defenders, UN Doc A/HRC/40/60 (10 January 2019)

Priority 6: Recognize that security must be understood holistically and that it encompasses physical safety, digital security, environmental security, economic stability, the freedom to practice cultural and religious beliefs and the mental and emotional well-being of women defenders and their families and loved ones.

101. The security of women defenders is multidimensional and should not be understood as physical safety alone. It is therefore critical for women defenders to be provided with multidimensional forms of support. In the face of online attacks and increased surveillance in particular, digital security has become increasingly important. Women defenders have also highlighted concerns about their economic security and their mental and emotional well-being.

102. Support should be provided to women defenders so that they are able to acquire knowledge and develop skills and capacities to conduct risk assessment and take mitigation measures, develop individual and collective security plans and protocols, deal with stigmatization, smear campaigns and online harassment, develop creative tactics and strategies for advocacy that lower the risks of retaliation and engage in practices for self- and collective care and well-being.

105. Funders should be attentive to the multidimensional security needs of women defenders. Women defenders should be given the support they need to take measures for their physical safety, digital security, economic security and mental and emotional well-being. Such support might include making provision for security measures, security training, training on software and hardware for digital security, legal aid, bail, emergency relocation, health insurance, pensions, social security and well-being-related activities.

108. The Special Rapporteur recommends that Member States: (d) Prioritize the protection of

women defenders in online spaces and adopt laws, policies and practices that protect their right to privacy and protect them from libel and hate speech;

109. The Special Rapporteur recommends that multilateral institutions, intergovernmental organizations and regional bodies: (f) Ensure that there is effective follow-up, implementation and accountability for recommendations to Member States concerning the security and protection of women defenders.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/29/32 (22 May 2015)

59. States should promote strong encryption and anonymity. National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online. Legislation and regulations protecting human rights defenders and journalists should also include provisions enabling access and providing support to use the technologies to secure their communications.

Concluding Observations on the Fourth Periodic Report of Paraguay, Human Rights Committee, UN Doc CCPR/C/PRY/CO/4 (20 August 2019)

36. […] The Committee is also concerned about allegations of the State's monitoring of private communications, including those of journalists. […]

37. The State party should: […] (c) Avoid State surveillance of any form, including of journalists and human rights defenders, except in the rare cases in which it is compatible with the Covenant, and establish a mechanism to oversee investigations of private communications carried out by the State; […]

Concluding Observations on the Fourth Periodic Report of Bulgaria, Human Rights Committee, UN Doc CCPR/C/BGR/CO/4 (15 November 2018)

33. […] the Committee remains concerned about the reported cases of illegal wiretapping of politicians, magistrates and journalists for the purpose of intimidation, and the lack of information regarding the remedies provided to them (arts. 14, 17, 21 and 24).

African Commission on Human and Peoples' Rights, Resolution on the Protection of Women Against Digital Violence in Africa, ACHPR/Res. 522 (LXXII) (11 August 2022)

The African Commission calls on States to: 9. Repeal vague and overly wide laws on surveillance as they contribute to the existing vulnerability of female journalists.

UN General Assembly Resolution on the Promotion and Protection of Human Right in the Context of Digital Technologies, UN Doc A/RES/78/213 (19 December 2023)

Noting with deep concern the use of technological tools developed by the private surveillance industry and by private or public actors to undertake surveillance, hacking of devices and systems, interception and disruption of communications, and data collection, interfering with the professional and private lives of individuals, including those engaged in the promotion and defence of human rights and fundamental freedoms, journalists and other media workers, in violation or abuse of their human rights,

17. *Emphasizes* that, in the digital age, encryption and anonymity tools have become vital for many journalists and media workers to freely exercise their work and their enjoyment of human rights, in

particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources, and calls upon States not to interfere with the use by journalists and media workers of such technologies and to ensure that any restrictions thereon comply with the obligations of States under international human rights law;

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)

Noting with deep concern also the use of technological tools developed by the private surveillance industry and by private or public actors to undertake surveillance, hacking of devices and systems, interception and disruption of communications, and data collection, interfering with the professional and private lives of individuals, including those engaged in the promotion and defence of human rights and fundamental freedoms, journalists and other media workers, in violation or abuse of their human rights, specifically the right to privacy,

12. *Emphasizes* that, in the digital age, encryption and anonymity tools have become vital for many journalists and media workers to freely exercise their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources, and calls upon States not to interfere with the use by journalists and media workers of such technologies and to ensure that any restrictions thereon comply with the obligations of States under international human rights law;

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

Noting with deep concern that, in many countries, persons and organizations engaged in promoting and defending human rights and fundamental freedoms, journalists and other media workers may frequently face threats and harassment and suffer insecurity, as well as unlawful or arbitrary interference with their right to privacy, as a result of their activities,

Noting with deep concern also the use of technological tools developed by the private surveillance industry by private or public actors to undertake surveillance, hacking of devices and systems, including through the use of malware or spyware, interception and disruption of communications, and data collection, interfering with the professional and private lives of individuals, including those engaged in the promotion and defence of human rights and fundamental freedoms, journalists and other media workers, in violation or abuse of their human rights, specifically the right to privacy,

8. *Calls upon* States: (n) To refrain from the use of surveillance technologies in a manner that is not compliant with international human rights obligations, including when used against human rights defenders, journalists and other media workers, and to take specific actions to protect against violations of the right to privacy, including by regulating the sale, transfer, use and export of surveillance technologies;

** See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021)*

UN Human Rights Council Resolution on Civil Society Space, UN Doc A/HRC/RES/53/13 (13 July 2023)

Recognizing that digital technologies have expanded the capacities of individuals and civil society groups to conduct their work, to advance human rights and to enable diverse and inclusive engagement, and recognizing also that the digital divide, digital surveillance and undue restrictions, such as Internet shutdowns and online censorship, are not conducive to a safe and enabling space for civil society,

UN Human Rights Council Resolution on the Situation of Human Rights in Myanmar, UN Doc A/HRC/RES/52/31 (4 April 2023)*

Expressing grave concern at the attacks against and the harassment of journalists and other media workers, including arbitrary arrests, enforced disappearance, torture and other ill-treatment, killings and surveillance, and Internet shutdowns and other restrictions on and interruptions to the Internet and social media, including the amendment to the law on television and radio broadcasting, and the proposed revival of the law on cybersecurity, which unnecessarily and disproportionately restricts the right to freedom of opinion and expression, including the freedom to seek, receive and impart information, the right to peaceful assembly and association and the right to privacy, as set forth in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights,

35. *Calls for* the protection of the rights to freedom of religion or belief, freedom of opinion and expression and freedom of peaceful assembly, and association and the right to privacy, as set forth in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, both online and offline, including by fully and permanently restoring all forms of Internet services across the country, lifting all forms of online censorship, including bans on access to the websites of media outlets and virtual private networks, halting all measures to implement online surveillance systems, including unlawful or arbitrary interception of communications, unlawful or arbitrary collection of personal data, unlawful or arbitrary hacking and the unlawful or arbitrary use of biometric technologies, repealing or reforming, in line with international human rights law and standards, all relevant legislation, including the Official Secrets Act, the Unlawful Associations Act, the Peaceful Assembly and Peaceful Procession Law, articles 66 (d), 68 (a), 77 and 80 (c) of the Telecommunications Act, the law on television and radio broadcasting, the Law Protecting the Privacy and Security of Citizens, the Electronic Transactions Law, articles 124A, 124C, 124D, 153, 295A, 499, 500, 505A, and 505 (a) and (b) of the Penal Code, and the Ward and Village Tract Administration Law, and enacting comprehensive data protection legislation;

** See also UN Human Rights Council Resolution on the Situation of human rights in Myanmar, UN Doc A/HRC/RES/49/23 (1 April 2022)*

UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/51/9 (6 October 2022)*

Equally concerned about incidents of the extraterritorial targeting of journalists and media workers, including killings, enforced disappearances, harassment and surveillance,

Recognizing that online attacks against women journalists, including through targeted unlawful or arbitrary digital surveillance, are one of the serious contemporary threats to their safety,

Emphasizing the particular risks with regard to the safety of journalists in the digital age, including the particular vulnerability of journalists to becoming targets of unlawful or arbitrary surveillance and/or the interception of communications, hacking, including government-sponsored hacking, malware, spyware, forced data handover or denial of service attacks to force the shutdown of particular media websites or services, in violation of their rights to privacy and to freedom of expression,

Emphasizing also that, in the digital age, encryption, pseudonymization and anonymity tools have become vital for many journalists to exercise freely their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources,

2. *Also condemns unequivocally* the extraterritorial targeting of journalists and media workers, including killings, enforced disappearances, harassment and surveillance, and urges States to cease and/or refrain from such attacks or measures;

11. *Calls upon* States:

(j) To protect in law and in practice the confidentiality of journalists' sources, including whistle-blowers, in acknowledgement of the essential role of journalists and those who provide them with information in fostering government accountability and an inclusive and peaceful society, subject only to limited and clearly defined exceptions provided in national legal frameworks, including judicial authorization, in compliance with States' obligations under international human rights law;

(l) To refrain from interference with the use of technologies such as encryption and anonymity tools, and from employing unlawful or arbitrary surveillance techniques, including through hacking;

** See also UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/45/18 (12 October 2020); UN Human Rights Council Resolution on the Safety of Journalists, A/HRC/RES/39/6 (27 September 2018); UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/33/2 (29 September 2016)*

UN Human Rights Council Resolution on Freedom of Opinion and Expression, UN Doc A/HRC/RES/50/15 (8 July 2022)

8. *Calls upon* all States: (j) To recognize that digital, media and information literacy includes risk awareness, digital security and self-protection training and guidance, and to acknowledge the particular risks of the digital age, including the particular vulnerability of journalists, other media workers and human right defenders to becoming targets of unlawful or arbitrary surveillance or interception of communications, in violation of their rights to privacy and to freedom of expression;

UN Human Rights Council Resolution on Recognizing the Contribution of Environmental Human Rights Defenders to the Enjoyment of Human Rights, Environmental Protection and Sustainable Development, UN Doc A/HRC/RES/40/11 (20 March 2019)

Gravely concerned that national security and counter-terrorism legislation and other measures, such as laws regulating civil society organizations, are in some instances misused to target human rights defenders or have hindered their work and endangered their safety in contravention of international law, and mindful that domestic law and administrative provisions and their application should not hinder but enable the work of human rights defenders, including by avoiding any criminalization, stigmatization, impediments, discrimination, obstructions or restrictions thereof contrary to the obligations and commitments of States under international human rights law,

7. *Calls upon* States to ensure that all legal provisions and their application affecting human rights defenders are clearly defined, determinable and non-retroactive in order to avoid potential abuse, to the detriment of fundamental freedoms and human rights, and specifically to ensure that the promotion and the protection of human rights are not criminalized, and that human rights defenders are not prevented from enjoying universal human rights owing to their work, whether they operate individually or in association with others;

UN Human Rights Council Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/RES/38/7 (5 July 2018)

Emphasizing the particular risks with regard to the safety of journalists in the digital age, including the particular vulnerability of journalists to becoming targets of unlawful or arbitrary surveillance and/or interception of communications, in violation of their rights to privacy and to freedom of expression,

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

20. […] Encryption and anonymity tools are widely used around the world, including by human rights defenders, civil society, journalists, whistle-blowers and political dissidents facing persecution and harassment. Weakening them jeopardizes the privacy of all users and exposes them to unlawful interferences not only by States, but also by non-State actors, including criminal networks. Such a widespread and indiscriminate impact is not compatible with the principle of proportionality (see A/HRC/29/32, para. 36).

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

18. […] While, in certain circumstances, intrusive surveillance measures may be permissible under articles 17 and 19 of the International Covenant on Civil and Political Rights on grounds of the protection of national security or public order, hacking can never be justified for political or business reasons, which is often the case when human rights defenders or journalists are targeted.

21. Encryption is a key enabler of privacy and security online and is essential for safeguarding rights, including the rights to freedom of opinion and expression, freedom of association and peaceful assembly, security, health and non-discrimination. […] In specific instances, journalists and human rights defenders cannot do their work without the protection of robust encryption, shielding their sources and sheltering them from the powerful actors under investigation. […]

28. […] where the rule of law is weak and human rights are under threat, the impact of client-side screening could be much broader, for example it could be used to suppress political debate or to target opposition figures, journalists and human rights defenders. Given the broad range of significant risks to human rights protection from mandated general client-side screening, such requirements should not be imposed without further substantial consideration of their potential human rights impacts and measures that mitigate those harms. Without in-depth investigation and analysis, it seems unlikely that such restrictions could be considered proportionate under international human rights law, even when imposed in pursuit of legitimate aims, given the severity of their possible consequences.

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

20. […] Encryption and anonymity provide individuals and groups with a zone of privacy online where they can hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks (A/HRC/29/32). Encryption and anonymity tools are widely used around the world, including by human rights defenders, civil society, journalists, whistle-blowers and political dissidents facing persecution and harassment. Weakening them jeopardizes the privacy of all users and exposes them to unlawful interferences not only by States, but also by non-State actors, including criminal networks. Such a widespread and indiscriminate impact is not compatible with the principle of proportionality (see A/HRC/29/32, para. 36).

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN Doc A/78/520 (10 October 2023)

47. […] Also identified was the use of legislation to create unnecessary burdens, restrict financing, introduce bureaucratic hurdles and even shut down civil society organizations, which "has the effect of limiting, restricting and controlling civil society", and the use of expansive security surveillance powers, which "creates incentives for self-censorship and directly undermines the ability of journalists and human rights defenders" (A/HRC/41/35, para. 26).

Report of the Working Group on Enforced and Involuntary Disappearances, 'New technologies and enforced disappearances', UN Doc A/HRC/54/22/Add.5 (11 September 2023)

14. In addition, international human rights mechanisms have been seized of cases where the use – or even the mere downloading – of a specific application (such as, for example, the messaging application ByLock) was considered by domestic authorities as the sole decisive evidence justifying mass arrests of human rights defenders and political opponents, in some cases leading to their subsequent enforced disappearance or death in custody. These cases are especially troublesome, due to, among others, the lack of clarity on the legal grounds invoked. Another issue of concern relates to the technologies and techniques used by domestic authorities to gather access to the servers, obtain IP addresses and the contents of users' exchanges, which might encompass hacking and infiltrating and stealing the data from the servers. […]

16. Instances of cyberattacks conducted against human rights defenders, including relatives of disappeared persons, encompass sabotage via phishing, malware and ransomware, espionage and supply of disinformation, as well as tainted leaks and doxxing. Often, those targeted are maliciously depicted or labelled as spies, foreign agents, terrorists or smugglers and this, in turn, exposes their accounts to special monitoring, suspension or hate campaigns, in a scenario that is characterised by under-reporting and policy and legal gaps and challenges in holding those responsible accountable, including because of the involvement of different jurisdictions. […]

57. The Working Group is especially concerned at the use of Internet shutdowns and targeted connectivity disruptions; spyware programmes; targeted and mass surveillance, including gait and facial-recognition; cyberattacks and Government- sponsored troll factories; and the specious use of technology-related legislation to suppress dissent and target human rights defenders and relatives of disappeared persons.

65. […] the Working Group recommends that States: (f) Take all measures to prevent cyberattacks, smearing and disinformation campaigns against human rights defenders, including relatives of disappeared persons, conducted through phishing, malware, ransomware, espionage, tainted leaks, troll farms and doxxing, and investigate all relevant instances with a view at identifying, prosecuting and sanctioning those responsible and offering redress to victims;

Report of the Special Rapporteur on the Independence of Judges and Lawyers, 'Reimagining justice: confronting contemporary challenges to the independence of judges and lawyers', UN Doc A/HRC/53/31 (13 April 2023)

52. […] Journalists and civil society actors must have open and secure access to online spaces, free from surveillance and censorship. […]

66. Intrusive measures by States and businesses enable surveillance that feeds analysis, prediction and even manipulation of behaviour, at times to the detriment of free and fair elections and democratic processes. Recent revelations about global abuses of spyware, targeting journalists, human rights defenders, dissidents, opposition politicians and diplomats, are in flagrant violation of the right to privacy and the protection of personal data. […]

Report of the Special Rapporteur on the Promotion and Protection of Human Rights while Counter-Terrorism, Human Rights Implications of the Development, Use, Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism, UN Doc A/HRC/52/39 (1 March 2023)

44. Sophisticated surveillance technology developed for counter-terrorism and national security purposes has increasingly become a focus of international concern thanks to a spate of revelations demonstrating that such tools are in fact being used to spy on politicians, journalists, human rights

activists, lawyers and ordinary citizens with no links to terrorism and who pose no national security threat. Intrusive covert technology for surveillance of the content of individuals' digital communications and other information, including metadata (location, duration, source and contacts) – commonly known as spyware – has proliferated internationally out of all control and poses substantial risks to the promotion and protection of human rights. […]

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 'Reinforcing media freedom and the safety of journalists in the digital age', UN Doc A/HRC/50/29 (20 April 2022)

43. Targeted electronic surveillance of journalists poses a challenge to investigative journalism, puts the confidentiality of journalistic sources at risk and exposes both journalists and their sources to increased physical harm. The full scale and impact of targeted surveillance of journalists is unknown given the lack of transparency surrounding the practice and the market that supports it; however, information that has come to light suggests it is used widely, in blatant disregard of international human rights law, with severe consequences for media freedom and the safety of journalists.

46. Women journalists have been disproportionately targeted in some countries and have experienced severe harm from targeted digital surveillance, which operates as a form of gender-based violence. Personal information of women journalists obtained through surveillance appear to have been used in online violence campaigns (including doxing).

47. Widespread digital surveillance practices ultimately discourage confidential sources from communicating with journalists, with significant chilling effects on whistle-blowing and investigative journalism. The extraterritorial reach of targeted digital surveillance allows States to control expression beyond their jurisdictions, possibly stifling investigative reporting at the global level. The use of targeted digital surveillance technologies against journalists to monitor the work they do is contrary to international human rights law, according to which both reporter and source enjoy rights that may be limited only in accordance with the strict requirements of article 19 (3) of the International Covenant on Civil and Political Rights.

49. States claim they require targeted digital surveillance technologies to prevent crime and terrorism, and companies such as NSO Group argue that the use of their surveillance tools is strictly limited to these purposes. However, extensive evidence has emerged of a broad parallel use by States of advanced surveillance technologies to target journalists whose work may be critical of Governments or focus on sensitive political or social issues. States have used targeted digital surveillance to limit investigative journalism, control public narratives, crack down on journalists and track journalists' sources, in violation of article 19 of the International Covenant.

122. The Special Rapporteur calls on the Human Rights Council and other relevant United Nations bodies to develop a consensus on impermissible targets of State cyberespionage and cyberattack. At a minimum, a presumption of protection from targeted digital surveillance and cyberattack should apply to journalists and media outlets.

123. States should incorporate adequate safeguards in national laws, such as judicial oversight, to ensure that digital surveillance laws and activities do not undermine international standards on the protection of journalists and their sources. They should hold surveillance companies accountable for foreseeable use of their technology by their clients to target journalists, and amend sovereign immunity laws to permit civil action against States engaged in cross-border digital attacks on journalists.

Report of the Special Rapporteur on the Human Rights of Migrants, Right to Freedom of Association of Migrants and Their Defenders, UN Doc A/HRC/44/42 (13 May 2020)

74. Even without an open criminal investigation or indictment against them, staff and volunteers of

civil society organizations that work with migrants have been subject to campaigns of government intimidation. These have included surveillance and intelligence gathering by law enforcement, targeted financial audits, unreasonable searches, prolonged detention at the border, discriminatory threats, travel restrictions and revocation of fast- track travel documents. […] It is reported that in 2019, journalists discovered that the United States authorities had put in place a confidential database of journalists and migrant advocates working at the United States/Mexico border and used the database, in coordination with the Mexican authorities, to monitor individuals on the list. A number of the individuals listed on the database – which included significant personal information about them – had alerts placed on their passports, causing them to be stopped and questioned for hours when attempting to cross borders."

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/43/52 (24 March 2020)

29. States and non-State actors should: (b) Meet legal obligations to protect the right to privacy and support the work of human rights defenders, regardless of their gender or that of those whose rights they are defending;

30. States should: (c) Establish supportive legal, institutional and administrative frameworks by: (v) Ensuring the privacy of communications of human rights defenders who engage with multilateral institutions and international and regional human rights bodies and promptly investigating any allegations of actions to the contrary; (vi) Ensuring that online media are not used to violate the rights to privacy of human rights defenders through, for example, the publication of private contact information by a third party, identity theft or threats of sexual violence.

Report of the Special Rapporteur on the Situation of Human Rights Defenders, Human Rights Defenders Operating in Conflict and Post-Conflict Situations, UN Doc A/HRC/43/51 (30 December 2019)

"34. Defenders' freedom of association continues to be curtailed in the name of public order, national security and counter-terrorism, often in contravention of both constitutional and international obligations. […] Surveillance, repeated administrative checks, raids of their premises and the seizure or damage of essential equipment add to this pressure. Defenders have also reported being the target of a growing number of digital attacks, paralyzing their communications means. […]"

Report of the Special Rapporteur on the Situation of Human Rights Defenders, UN Doc A/74/159 (15 July 2019)

"21. In addition, attacks such as blocking web pages, blocking network data traffic, denial of services (online streaming, for example), remote attacks to take control of equipment or extract information, use of malicious programmes (malware) to monitor and track communications, hacking accounts for theft of credentials, identity theft (phishing), blocking of profiles, creation of fake profiles or arbitrary removal of content by digital platforms are some of the ways in which many rights of human rights defenders are violated (A/HRC/17/27 and A/HRC/41/35).

82. [The lack of adequate resources and capacities] is particularly evident in cases of digital attacks that require complex investigations. According to a recent report by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/41/35), most States have the recourses to acquire technology that can be used in digital attacks on human rights defenders. However, the existence of legislation restricting access to public information and the lack of independent accountability mechanisms makes it impossible to determine how the acquired technology is being used, let alone establishing responsibility."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and

Fundamental Freedoms While Countering Terrorism, Impact of Measures to Address Terrorism and Violent Extremism on Civic Space and the Rights of Civil Society Actors and Human Rights Defenders, UN Doc A/HRC/40/52 (1 March 2019)

8. In many parts of the world, any form of expression that articulates a view contrary to the official position of the State, addresses human rights violations and comments on ways to do things better, in accordance with international human rights obligations, constitutes a form of terrorist activity or violent extremism or a broad "threat to national security", which often encompasses both terrorism and extremism. No region of the world is immune from this trend. In some regions, the instrumentalization of counter-terrorism, the prevention and countering of violent extremism, and protection of national security measures is brutal, with members of civil society arrested and detained on spurious grounds, with some States even using counter-terrorism laws to silence defenders of the rights of lesbian, gay, bisexual, transgender and intersex persons, and others surveilling individuals involved in peaceful protests against climate change and linking them to terrorism investigations or branding them as "ecoterrorists". Journalists have been particularly targeted by counter-terrorism and extensive security legislation.

27. Enjoyment of the rights to privacy and to freedom of expression are closely interrelated. Undue interference with the right to privacy limits the free development and exchange of ideas, and can have a chilling effect on freedom of expression. Civil society may refrain from online exchange, for fear of attracting government interest. Restrictions have a particularly negative impact on journalists and human rights defenders who fear accusations of "spreading terrorist propaganda".

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/20/17 (4 June 2012)

63. Additionally, the Special Rapporteur is deeply concerned by harassment of online journalists and bloggers, such as illegal hacking into their accounts, monitoring of their online activities... and the blocking of websites that contain information that are critical of authorities. Such actions constitute intimidation and censorship.

64. The Special Rapporteur reiterates that the right to freedom of expression should be fully guaranteed online, as with offline content. If there is any limitation to the enjoyment of this right exercised through the internet, it must also conform to the criteria listed in article 19, paragraph 3, of the International Covenant on Civil and Political Rights. This means that any restriction imposed as an exceptional measure must (i) be provided by law, which is clear and accessible to everyone; (ii) pursue one of the legitimate purposes set out in article 19, paragraph 3, of the Covenant; and (iii) be proven as necessary and the least restrictive means required to achieved the purported aim.

Concluding Observations on the Fourth Periodic Report of the Islamic Republic of Iran, Human Rights Committee, UN Doc CCPR/C/IRN/CO/4 (26 October 2023)

45. The Committee is concerned about reports of targeted surveillance and monitoring of individuals, in particular human rights defenders, journalists and activists, and regrets the lack of information on the legal safeguards applied in the surveillance regime. […]

Concluding Observations on the Eighth Periodic Report of Colombia, UN Doc CCPR/C/COL/CO/8 (21 July 2023)

30. The Committee notes with concern the illegal surveillance activities allegedly conducted against human rights defenders and journalists, as well as the monitoring of social media by the Integrated Cybersecurity Command in the context of social protests. The Committee also regrets the lack of information provided by the State party in this regard (art. 17).

Concluding Observations on the Second Periodic Report of Uganda, Human Rights

Committee, UN Doc CCPR/C/UGA/CO/2 (20 July 2023)

16. […] The Committee is further concerned that the definition of terrorism contained in articles 7 and 9 of the Act is overly broad and has been used to prosecute and suppress the work of journalists, political opponents and civil society organizations (arts. 2, 6, 9, 14, 15, 17, 19 and 22).

Report of the Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, The Guiding Principles on Business and Human Rights: Guidance on Ensuring Respect for Human Rights Defenders, UN Doc A/HRC/47/39/Add.2 (22 June 2021)

22. […] The types of risks faced by human rights defenders when highlighting irresponsible practices involving business enterprises or their business partners (including actors with links to governments) include threats, or the reality, of: smears, slurs, harassment, intimidation, surveillance, strategic lawsuits against public participation (SLAPPs), criminalisation of their lawful activities, physical attacks and death.

50. Illustrative actions that States should take: […] provide guidance to business enterprises to assist them in trying to prevent their products or services with surveillance capabilities from being misused by others to commit human rights abuses.

104. States, business enterprises, and development finance institutions investing in and/or implementing development projects, may find themselves linked to, or complicit in human rights abuses targeting defenders due to engaging in, or reacting to, conflicts that target human rights defenders. For example, in order to facilitate business access to an area, or the advancement of a project. In other contexts, they may be involved in shutting down protests, conducting surveillance on defenders, or restricting trade union activity.

109. The use of products developed by technology companies, including in surveillance by business enterprises and by States, can severely restrict the rights of human rights defenders and endanger, and harm defenders themselves. All technology companies should resist any demands to restrict, or collude in restricting, human rights, especially the right to privacy, and the freedoms of expression, and of assembly and association. Human rights defenders ought not to be tracked or be put under surveillance when using the technology they rely on to do their work. They need to be supported in taking measures to protect themselves and business enterprises that understand and respect the work that human rights defenders do can play a vital role in sharing knowledge about the technology they have created.

African Commission on Human and Peoples' Rights, Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa, ACHPR/Res.573 (LXXVII) (9 November 2023)

Noting Principle 20 of the Declaration which calls on States to guarantee the safety of journalists and other media practitioners and in particular, take measures to prevent attacks on them, including threats and unlawful surveillance undertaken by State and non-State actors;

Concerned about the prevalence of mass surveillance and unlawful targeted communication surveillance that does not conform with international human rights law and standards, and the disproportionate targeting of journalists, human rights defenders, civil society organizations, whistleblowers and opposition political activists, without appropriate safeguards for privacy rights;

***Khadija Ismayilova v Azerbaijan*, Apps Nos 65286/13 and 57270/14, Judgment, European Court of Human Rights (10 January 2019)**

4. Moreover, the Court has repeatedly stressed that interference with freedom of expression may

have a "chilling effect" on the exercise of that freedom (see, among other authorities, *Baka Hungary* [GC], no 20261/12, § 160, 23 June 2016), and this is more so in cases of serious crimes committed against journalists, making it of utmost importance for the authorities to check a possible connection between the crime and the journalist's professional activity (see *Huseynova*, cited above, § 115, and *Mazepa and Others*, cited above, § 73).

110. In respect of the negative obligation, [the applicant] argued that there had been an unjustified interference with her Article 8 rights by persons or entities that could be considered "State agents", undermining respect for her private life and connected to her journalistic investigative work concerning alleged corruption by the President's family.

111. However, having regard to the applicant's arguments in support of the alleged breach of the negative obligation (see, in particular, paragraphs 86-91 above), the Court considers that they are based either on circumstantial evidence or on assertions requiring corroboration and further investigation. While the Court must remain sensitive to the potential evidentiary difficulties encountered by a party, it has not been possible, on the basis of the material available, to establish in the present case to the requisite standard of proof, "beyond reasonable doubt" (see *Nuri Kurt v. Turkey*, no 37038/97, § 101, 29 November 2005), that there was unjustified interference attributable to the State.

112. The Court reiterates that, although the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life. […]

116. The Court considers that the acts complained of were grave and an affront to human dignity: an intrusion into the applicant's home in the form of unauthorised entry into her flat and installation of wires and hidden video cameras inside the flat; a serious, flagrant and extraordinarily intense invasion of her private life in the form of unauthorised filming of the most intimate aspects of her private life, which had taken place in the sanctity of her home, and subsequent public dissemination of those video images; and receipt of a letter threatening her with public humiliation. Furthermore, the applicant is a well-known journalist and there was a plausible link between her professional activity and the aforementioned intrusions, whose purpose was to silence her.

117. […] the Court considers that practical and effective protection of the applicant required that effective steps be taken in the framework of the criminal investigation with a view to identifying and prosecuting the perpetrator or perpetrators of those acts.

118. For an investigation to be regarded as "effective", it should in principle be capable of leading to the establishment of the facts of the case and to the identification and punishment of those responsible. This is not an obligation of result, but one of means. […] the Court has previously used the "significant flaw" test. The Court's task under that test is to determine whether the alleged shortcomings in the investigation had such significant flaws as to amount to a breach of the respondent State's positive obligations under Article 8 of the Convention.

119. […] In a situation where the applicant was well known in society specifically for her journalistic activity and for that activity only, it is difficult to discern any motive for threats of public humiliation received by her other than a motive connected to that activity. The absence of such a motive could be demonstrated only if it was conclusively and convincingly ruled out as a result of an effective investigation.

131. Having regard to the significant flaws in the manner in which the authorities investigated the case, as well as the overall length of the proceedings, the Court finds that the authorities failed to comply with their positive obligation to ensure the adequate protection of the applicant's private life by carrying out an effective criminal investigation into the very serious interferences with her private

life. […]"

162. The applicant in the present case is a well-known investigative journalist who has received a number of international awards. As noted above, the acts of a criminal nature committed against the applicant were apparently linked to her journalistic activity; no other plausible motive for the harassment she had to face has been advanced or can be discerned from the case file (see paragraph 119 above).

164. In such circumstances, having regard to the reports on the general situation concerning freedom of expression in the country and the particular circumstances of the present case, the Court considers that the threat of public humiliation and the acts resulting in the flagrant and unjustified invasion of the applicant's privacy were either linked to her journalistic activity or should have been treated by the authorities when investigating as if they might have been so linked. In this situation Article 10 of the Convention required the respondent State to take positive measures to protect the applicant's journalistic freedom of expression, in addition to its positive obligation under Article 8 of the Convention to protect her from intrusion into her private life.

Annual Report of the Inter-American Commission on Human Rights 2020, Volume II – Annual Report of the Office of the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II Doc 28 (30 March 2021)

In view of the region's ongoing challenges that have been highlighted in this report, the Office of the Special Rapporteur for Freedom of Expression makes the following recommendations to the member states of the OAS: (10) Adopt or adapt and effectively implement supplemental laws and regulations to guarantee, in law and in practice, the right of journalists and persons professionally engaged in the gathering and dissemination of information to the public through any media the protection of the identity of their sources of confidential information from direct and indirect exposure, including interference through surveillance.

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Concern Over the Acquisition and Implementation of Surveillance Programs by States of the Hemisphere, Press Release R80/15 (21 July 2015)

This Office has stated that the surveillance of communications and the interference in privacy that exceeds what is stipulated by law, which are oriented to aims that differ from those which the law permits or are carried out clandestinely, must be harshly punished. Such illegitimate interference includes actions taken for political reasons against journalists and independent media.

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet OEA/Ser.L/V/II. CIDH/RELE/INF.11/13 (31 December 2013)

158. The ideological basis of all these regimes was the 'National Security Doctrine,' which regarded leftist movements and other groups as 'common enemies'." Even today, it has been reported that national security reasons tend to be invoked to place human rights defenders, journalists, members of the media, and activists under surveillance, or to justify excessive secrecy in the decision-making processes and investigations tied to surveillance issues. Clearly, this kind of interpretation of the "national security" objective cannot be the basis for the establishment of surveillance programs of any kind, including, naturally, online communications surveillance programs.

D. PROTEST SURVEILLANCE

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc

A/HRC/RES/54/21 (12 October 2023)*

Reaffirming the human right to privacy […] and recognizing that the exercise of the right to privacy is important for the realization of other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association, and is one of the foundations of a democratic society,

** See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021)*

UN Human Rights Council Resolution on the Promotion and Protection of Human Rights in the Context of Peaceful Protests, UN Doc A/HRC/RES/50/21 (8 July 2022)*

Expressing its concern also at the arbitrary and unlawful surveillance, both in physical spaces and online, of individuals engaged in peaceful protests, including through the use of closed-circuit television and aerial surveillance vehicles, as well as through the use of new and emerging digital tracking tools, such as biometric technologies, including facial and emotional recognition and international mobile subscriber identity-catchers ("stingrays"),

Emphasizing that technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity online, are important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association,

28. *Calls upon* States to refrain from the use of digital technology to silence, arbitrarily or unlawfully surveil, or harass individuals or groups solely for having organized, taken part in or observed, monitored or recorded peaceful protests, or from ordering blanket Internet shutdowns and from blocking websites and platforms including around protests or key political moments;

29. *Urges* States to refrain from the arbitrary or unlawful use of biometric identification technologies, including facial recognition, to identify those peacefully participating in an assembly;

30. *Calls upon* States to refrain, in accordance with applicable national procedures and international norms and standards, from the export, sale or transfer of surveillance goods and technologies and less-lethal weapons when they assess that there are reasonable grounds to suspect that such goods, technologies or weapons might be used to violate or abuse human rights, including in the context of assemblies;

31. *Expresses grave concern* at the use of private surveillance technologies to commit widespread violations and abuses against those exercising their right to peaceful assembly, including through hacking;

32. *Calls upon* States to refrain from applying any undue restrictions to technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity online, given that these are important to ensure the enjoyment of human rights, in particular the rights to privacy, in the context of assemblies;

** See also UN Human Rights Council Resolution on the Promotion and Protection of Human Rights in the Context of Peaceful Protests, UN Doc A/HRC/RES/44/20 (23 July 2020);*

UN Human Rights Council Resolution on the Rights to Freedom of Peaceful Assembly and of Association, UN Doc A/HRC/RES/50/17 (8 July 2022)

10. *Also calls upon* States to refrain from […] the use of digital technology to silence, unlawfully or arbitrarily surveil or harass individuals or groups for having organized, taken part in or observed, monitored or recorded peaceful assemblies, […]

Report of the United Nations High Commissioner for Human Rights, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests, UN Doc A/HRC/44/24 (24 June 2020)

8. […] Messaging and social networking platforms that use encryption technology to prevent monitoring enhance the security of civil society groups' digital communication, while also providing tools specifically geared to network organizing at the grass-roots level. To protect the safety of communications, some messaging platforms have adopted the use of end-to-end encryption.

12. The use of body cameras by security officials can also help to ensure transparency and accountability for violence or human rights violations. […] The special procedure mandate holders warned that a delicate balancing of potential intrusions into privacy should be considered (see paras. 16–23 below).

13. […] Moreover, there are also responsibilities for the social media companies that control online spaces, particularly with regard to encryption, content moderation, and algorithmic amplification […].

24. Safe and confidential communications play a key role in the planning and holding of peaceful protests. Technology-enabled surveillance poses significant risks to the enjoyment of human rights in peaceful assemblies and is an important contributor to the shrinking of civic space in many countries. New technologies have significantly expanded the abilities of State authorities to surveil protests, protest organizers and participants. These technologies are used to monitor the planning and organization of protests – for example, through the hacking of the digital tools used by those seeking to assemble. They are also used to conduct surveillance during protests – for example, through the use of biometrics-based facial recognition technology and the interception of communications. In response to this trend, the Human Rights Council has underlined the importance of privacy online for the realization of the rights of peaceful assembly and association. It has also emphasized that technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption and anonymity, can be important to ensure the enjoyment of these rights. In her report on the right to privacy in the digital age, the High Commissioner outlined key safeguards that States should implement for surveillance measures. National legal frameworks, based on the principles of necessity and proportionality, are needed to regulate the use of surveillance tools.

25. Similarly, the Special Rapporteur on the right to freedom of opinion and expression has called for strict limitations on restrictions to encryption and anonymity in order to ensure compliance with the principles of legality, necessity, proportionality and legitimacy. Such restrictions are often used by law enforcement and intelligence agencies as quick reactions to terrorism, while failing to meet imperatives of necessity and proportionality, and consequently undermining trust in the rule of law. Other experts have recalled the importance of judicial control and proportionality when anonymity is lifted.

26. The Special Rapporteur on the rights to freedom of peaceful assembly and of association has called for the prohibition of indiscriminate and untargeted surveillance of those exercising their right of peaceful assembly, in both physical and digital spaces. He underscored that surveillance of protesters should only be conducted on a targeted basis, and only when there is reasonable suspicion that they are engaging in or planning to engage in serious criminal offences, based on principles of necessity and proportionality and with judicial supervision. The General Assembly has also recognized that States should refrain from employing unlawful or arbitrary surveillance

techniques, which could include forms of hacking.

27. Despite these warnings, States continue to unduly resort to intrusive online surveillance and the hacking of the ICT tools used by those planning or organizing protests as well as protesters themselves. Surveillance software is used to infiltrate protesters smartphones, often after they are duped into downloading certain applications. These applications give unimpeded access to protesters' phones and their contacts, chat messages, phone conversations, and photos and videos shared on social media and communication platforms. Another cause for concern is the hacking of the social media accounts of protesters and organizers. Some State authorities use hacked devices to create false accounts to impersonate protest organizers and spread false information, or endanger followers, including through doxing (i.e., maliciously publishing personal information to encourage physical harm to protesters and organizers).

29. Online surveillance technologies and interference in communications often lead to harassment and intimidation.

30. Another development that is particularly problematic is the practice of routinely making audiovisual recordings of assembly participants, often in combination with the deployment of facial recognition technology.

31. The use of facial recognition technology brings about significant risks for the enjoyment of human rights, including the right of peaceful assembly. Despite remarkable accuracy gains in recent years, this technology is still prone to errors. For example, an image may be falsely considered a match (known as a "false positive"), with significant consequences to a person's rights, including in cases where a person is wrongly flagged as a suspect of a crime and may be detained and prosecuted. When facial recognition technology is used on a large number of people, even low rates of error may result in the inaccurate flagging of hundreds of individuals.

33. The use of facial recognition technology to identify persons in the context of assemblies has considerable adverse effects on the rights to privacy, freedom of expression and peaceful assembly, if effective safeguards are not in place. A person's image constitutes one of the key attributes of her or his personality as it reveals unique characteristics distinguishing her or him from other persons. Recording, analysing and retaining someone's facial images without her or his consent constitute interferences with a person's right to privacy. By deploying facial recognition technology at assemblies, these interferences occur on a mass and indiscriminate scale, as this requires the collection and processing of facial images of all persons captured by the camera equipped with or connected to a facial recognition technology system.

35. Audiovisual recording and facial recognition techniques should only be used when such measures meet the three-part test of legality, necessity and proportionality. The possibility that recourse to facial recognition technology during peaceful protests could ever meet the test of necessity and proportionality, given its intrusiveness and serious chilling effects, has been questioned. Authorities should generally refrain from recording assembly participants. As required by the need to show proportionality, exceptions should only be considered when there are concrete indications that serious criminal offences are actually taking place or that there is cause to suspect imminent and serious criminal behaviour, such as violence or the use of firearms. Existing recordings should only be used for the identification of assembly participants who are suspects of serious crimes.

36. While the use of facial recognition technology in the context of peaceful assemblies is discouraged, governments that still deploy this technology should ensure that they do so on a clear legal basis, including a robust, human rights-compliant regulatory framework. Measures should provide for the immediate deletion of all data, except for the specific segments that may be necessary for the conduct of criminal investigations and the prosecution of violent crimes. All

persons concerned should have the right to access and to request the rectification and expungement of such information that is stored without a legitimate purpose and a legal basis, except when this would frustrate criminal investigations or prosecutions for which these data are needed.

37. Furthermore, any use of audiovisual recording and facial recognition technology must be subject to robust and well-resourced oversight mechanisms. In any case, any use of recording and facial recognition technology should be open to judicial challenge. In all circumstances, the authorities should be transparent about the use of recording and facial recognition technology and always notify members of the public when they are, or may be, recorded and/or when their images may be processed in a facial recognition system.

39. The use of surveillance technologies has grown rapidly over recent years with the support of the private sector. All business enterprises, including those that develop new technologies that are used to monitor the activities of civil society actors, have a responsibility to respect human rights, […].

40. […] States should refrain from granting export licences, if there are indications that the surveillance tools at issue could be used in the importing country to violate or abuse human rights. Against the background of widespread abuse of surveillance technologies around the world, the Special Rapporteur on the right to freedom of opinion and expression has called for States to impose a moratorium on granting export licences for surveillance technologies until the use of those technologies can be technically restricted to lawful purposes that are consistent with human rights standards, or until it can be ensured that those technologies will only be exported to countries in which their use is subject to authorization – granted in accordance with due process and the standards of legality, necessity and legitimacy – by an independent and impartial judicial body. The High Commissioner supports this call.

53. In this context, the High Commissioner recommends that States:

(d) Ensure that any interference with the right to privacy, including by communications surveillance and intelligence-sharing, complies with international human rights law, including the principles of legality, necessity and proportionality;

(e) Promote and protect strong encryption and anonymity options online, and ensure that laws provide for judicial supervision for any lifting of anonymity;

(f) Prohibit the use of surveillance techniques for the indiscriminate and untargeted surveillance of those exercising the right of peaceful assembly and association, both in physical spaces and online, and ensure that targeted surveillance measures are authorized only when there is reasonable suspicion that a particular individual has committed or is committing a criminal offence, or is engaged in acts amounting to a specific threat to national security;

(h) Never use facial recognition technology to identify those peacefully participating in an assembly;

(i) Refrain from recording footage of assembly participants, unless there are concrete indications that participants are engaging in, or will engage in, serious criminal activity, and such recording is provided by law, with the necessary robust safeguards;"

(j) Establish a moratorium on the use of facial recognition technology in the context of peaceful assemblies, at least until the authorities responsible can demonstrate compliance with privacy and data protection standards as well as the absence of significant accuracy issues and discriminatory impacts, and until the following recommendations are implemented:

(i) Systematically conduct human rights due diligence before deploying facial recognition technology devices and throughout the entire life cycle of the tools deployed;
(ii) Establish effective, independent and impartial oversight mechanisms for the use of facial recognition technology, such as independent data protection authorities, and consider imposing a requirement of prior authorization by an independent body for the use of facial recognition technologies in the context of assemblies;
(iii) Put in place strict privacy and data protection laws that regulate the collection, retention, analysis and otherwise processing of personal data, including facial templates;
(iv) Ensure transparency about the use of image recordings and facial recognition technology in the context of assemblies, including through informed consultations with the public, experts and civil society, and the provision of information regarding the acquisition of facial recognition technology, the suppliers of such technology and the accuracy of the tools;
(v) When relying on private companies to procure or deploy these facial recognition technologies, request that companies carry out human rights due diligence to identify, prevent, mitigate and address potential and actual adverse impact on human rights and, in particular, ensure that data protection and non-discrimination requirements be included in the design and the implementation of these technologies;

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, UN Doc A/HRC/41/41 (17 May 2019)

12. While these rights are not absolute, the freedom to access and use digital technologies for the exercise of peaceful assembly and association rights should be viewed as the rule, and the limitations as the exception. The general norm should be to permit the open and free use of the Internet and other digital tools. Resolution 15/21 of the Human Rights Council makes it clear that to be permissible restrictions should be "prescribed by law and which are necessary in a democratic society in the interests of national security or public safety, public order (*ordre public*), the protection of public health or morals or the protection of the rights and freedoms of others". Where such restrictions are made, "States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights. In no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right.

14. In the digital age, the positive obligation to facilitate the exercise of the rights to freedom of peaceful assembly and of association includes efforts "to bridge the digital divides, including the gender digital divide, and to enhance the use of information and communications technology, in order to promote the full enjoyment of human rights for all". The obligation to protect requires that positive measures be taken to prevent actions by non-State actors, including businesses, that could unduly interfere with the rights to freedom of peaceful assembly and of association.

15. Where peaceful assembly and association rights are unduly restricted, the victim(s) should be able to exercise their rights to an effective remedy and obtain redress. The Human Rights Council has called on States to "ensure effective remedies for human rights violations, including those related to the Internet, in accordance with their international obligations".

24. Encryption technologies, pseudonymity and other security features have enabled individuals belonging to minority groups to find one another and create community. The Human Rights Council has stressed that "technical solutions to secure and protect the confidentiality of digital communications, including measures for encryption and anonymity, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association". The Special Rapporteur asserts that the same is true for the organization and conduct of associations. These tools provide individuals and civil society actors with safe online space to gather and connect with other members of their group as well as to organize and coordinate activities, without undue interference from third parties and

government.

29. […] Numerous jurisdictions have resorted to shutting down access to communications networks and services during elections and public demonstrations, and blocking websites belonging to civil society groups, including human rights organizations. Demonstrating a sophisticated grasp of emerging technical tools, some States – and malicious third-party actors – have increased use of digital surveillance and online harassment against civil society actors, human rights defenders, opposition political leaders and those who plan to stage peaceful public assemblies. […]

35. Mandate holders have stressed that overly broad and vague surveillance laws often fail to target specific individuals on the basis of a reasonable suspicion. For example, the Investigatory Powers Act 2016, of the United Kingdom of Great Britain and Northern Ireland, contained vague language that allowed authorities to target a group or category of people without requiring each target of the surveillance to be individually identified. Other forms of surveillance law give enormous licence to States to monitor citizens' online activities, such as the Telecommunications and Other Legislation Amendment Bill, of Australia, which includes provisions that would grant authorities unfettered powers to compel companies to facilitate access to encrypted user data for security agencies and weaken encryption technologies. The risks of abuse are increased given that many existing laws and regulations governing surveillance do not keep pace with rapid changes in surveillance technology and its potential uses.

43. Some States have harnessed technology to monitor and hamper the work of human rights defenders and civil society actors. Tactics are varied. Many involve hacking phones and computers, issuing death and rape threats, disseminating doctored images, temporarily suspended targets' accounts, hijacking hashtags, spreading conspiracy theories, accusations of treason and promoting virulently discriminatory sentiments. While the Special Rapporteur is mindful that States are not the only perpetrators of these acts, government responsibility for these acts extends into the commissioning and encouragement of such conduct by third parties.

46. The use of commercial spyware, such as FinFisher monitoring technology and the Pegasus spyware suite, to launch cyberattacks against civil society actors is another example of this trend. Well-documented reports have linked the Pegasus spyware suite to spyware attacks against activists and human rights defenders in Bahrain, Kazakhstan, Mexico, Morocco, Saudi Arabia and the United Arab Emirates, among others. These attacks allow hacking into, and watching in real time, their communications, location and activities, and can affect targets both within a State or extraterritorially.

47. Infiltrating social media groups or forums and tracking the online activities of civil society by "friending" activists is another technique used. Open source intelligence can also allow for the pre-emptive disruption of peaceful protests by arresting organizers who are communicating and planning their activities online.

48. Women and lesbian, gay, bisexual, transgender and intersex persons are at particular risk of facing these attacks. For example, the Government of Egypt reportedly identified and arrested lesbian, gay, bisexual, transgender and intersex activists by infiltrating and surveilling their activities on social media platform Grindr. Authorities in Brazil used Tinder to form relationships and then conduct surveillance on women activists engaged in protests. In Thailand, women human rights defenders were subjected to extensive discrediting, harassment campaigns and death threats in blogs and on social media. These attacks take particular forms, which include the dissemination of doctored pictures, usually of a sexualized and gendered nature; the spreading of information designed to discredit, often full of harmful and negative gender stereotypes; violent hate messages and threatening messages on social networks, including calls for gang rape and for murder; and breaches of privacy, including hacking into family members' computers and

phones and exposing the phone number, the home address and personal and family photos. The mandate holder echoes the findings of the Special Rapporteur on violence against women, its causes and consequences, that online abuse against women is a direct attack on women's visibility and full participation in public life, and should be duly investigated and punished.

55. The necessity requirement implies demonstrating how surveillance would achieve a stated purpose, something often jeopardized by the very act of surveillance. As stated by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, "there is widespread consensus among information security experts that such vulnerabilities impose significant costs on digital security overall, as they may be exploitable by unauthorized third parties even if they are intended solely for government access.

56. The proportionality principle requires proof that the measure used is the least invasive option. Mass surveillance or bulk collection and analysis of all communications metadata – explicitly designed to target associations between individuals – is inherently disproportionate. Similarly, legal requirements on communications service providers to store personal and sensitive data locally and register SIM cards on an indiscriminate basis allow authorities to access information which is not relevant and material to any serious crime or specific threat. […] Similarly, International Mobile Subscriber Identity capture devices (IMSI catchers) allow countries to collect data from thousands of mobile phones in a specific area, or at public events such as political demonstrations. Such practices are used to identify and surveil all individuals who participate in a particular event or are present in a certain public space. These forms of identification and data collection violate the individual's anonymity in public spaces and exert significant "chilling effects" on decisions to participate in public gatherings.

57. The use of surveillance techniques for the indiscriminate and untargeted surveillance of those exercising their right to peaceful assembly and association, in both physical and digital spaces, should be prohibited. Surveillance against individuals exercising their rights of peaceful assembly and association can only be conducted on a targeted basis, where there is a reasonable suspicion that they are engaging in or planning to engage in serious criminal offences, and under the very strictest rules, operating on principles of necessity and proportionality and providing for close judicial supervision.

58. By virtue of their control of online platforms and tools, these companies are liable to States' requests for access to users' data. At times, such demands may come in the form of informal requests or pressure. Where domestic laws are in violation of international human rights standards and norms, companies are confronted with competing legal obligations that threaten their compliance with human rights as well as their ability to operate in certain jurisdictions. This may result in infringement of users' rights to peaceful assembly and association, and raises questions regarding transparency and accountability. […]

61. Policies and features on user privacy and security of communications can also affect the enjoyment of the rights of peaceful assembly and association. Only a few digital technology companies allow the use of pseudonyms or other ways to mask an individual's identity, or provide for encrypted communications. […]

63. […] States should adopt and enforce laws and policies that focus on creating mandatory requirements for digital technology companies to exercise due diligence to identify, prevent, mitigate, and account for how they address, human rights impacts of their business and products, as well as for robust transparency and remediation mechanisms. […]

64. The Special Rapporteur believes the international human rights law framework should govern digital technology companies' responses to government requests, content moderation and engineering choices, including computational curation of content. This means that standards of

legality, necessity and legitimacy should be applicable to companies' decisions that affect peaceful assembly and association rights. […]

67. States should ensure that the rights of peaceful assembly and association are respected, protected and implemented in national legal frameworks, policies and practices, in accordance with international law. Digital technology companies must commit to respect freedoms of peaceful assembly and association and carry out due diligence to ensure that they do not cause, contribute to or become complicit in violation of these rights. In fulfilling their respective responsibilities, States and digital technology companies should comply with well-established principles of non-discrimination, pluralism of views, transparency, multi-stakeholder participation, and access to justice.

69. States should ensure that any interference with the rights to freedom of peaceful assembly and of association is "prescribed by law" and is "necessary in a democratic society in the interests of national security or public safety, public order (*ordre public*), the protection of public health or morals or the protection of the rights and freedoms of others". Restrictions on grounds of "national security", "public safety" and "protection of morals" should be clearly and narrowly defined, so as to prevent their abuse by authorities.

73. States should create an enabling legal framework for the right to peaceful assembly and association in the digital age, by:
(c) Revising and amending cybercrime, surveillance and antiterrorism laws and bringing them into compliance with international human rights norms and standards governing the right to privacy, the right to freedom of opinion and expression, the right to freedom of peaceful assembly and the right to freedom of association;
(d) Promoting and protecting strong encryption and anonymity, including by adopting laws, regulations and policies that confer only on courts the power to remove the right to anonymity, rather than on law enforcement agencies.

76. Prohibit the use of surveillance techniques for the indiscriminate and untargeted surveillance of those exercising the right to peaceful assembly and association, both in physical spaces and online.

77. Refrain from unduly conducting targeted surveillance using digital tools against civil society actors, protest organizers, minorities and others seeking to exercise their rights to freedom of peaceful assembly and of association. In order to be permissible, targeted surveillance may occur only on the basis that such activities are adopted openly; are time-limited; operate in accordance with established international standards of legal prescription, legitimate aim, necessity and proportionality; and are subjected to continued independent supervision that includes robust mechanisms for prior authorization, operational oversight and review. Individuals and groups should be notified if their rights are breached by surveillance, and effective remedies should be guaranteed.

78. Any application of new forms of technological surveillance should also adhere to the above-mentioned principles and standards – including surveillance conducted extraterritorially. States should set up independent inquiries to examine the use of any surveillance technologies, so that the public can assess the manner and frequency of their use, the justifications for and the necessity and proportionality of that use, and whether such technologies are being used in an improper or overly broad way.

84. Companies should seek to prevent or mitigate the adverse human rights impacts of their involvement, to the maximum extent allowed by law, whenever they are requested by States to censor, surveil or monitor individuals or groups or to make available data that they collect, process or retain.

85. Companies should recognize international human rights law as the authoritative framework for ensuring that peaceful assembly and association rights are respected in their products and services and should evaluate their policies accordingly. Companies should ensure that their policies and community guidelines are sufficiently clear, accessible and in keeping with international human rights standards. They should also provide more detailed examples or case studies of the way in which their community standards are applied in practice, so that users can understand the circumstances under which personal data or information may be accessed, content may be restricted, or access to the service may be blocked or restricted.

UN Human Rights Committee, General Comment No 37 (2020) on the Right of Peaceful Assembly (Article 21), UN Doc CCPR/C/GC/37 (17 September 2020)

6. Article 21 of the Covenant protects peaceful assemblies wherever they take place: outdoors, indoors and online; in public and private spaces; or a combination thereof. […]

10. The way in which assemblies are conducted and their context changes over time. This may in turn affect how they are approached by the authorities. For example, given that emerging communications technologies offer the opportunity to assemble either wholly or partly online and often play an integral role in organizing, participating in and monitoring physical gatherings, interference with such communications can impede assemblies. While surveillance technologies can be used to detect threats of violence and thus to protect the public, they can also infringe on the right to privacy and other rights of participants and bystanders and have a chilling effect.

13. […] Although the exercise of the right of peaceful assembly is normally understood to pertain to the physical gathering of persons, article 21 protection also extends to remote participation in, and organization of, assemblies, for example online.

34. […] States should ensure that the activities of Internet service providers and intermediaries do not unduly restrict assemblies or the privacy of assembly participants. […]

60. The wearing of face coverings or other disguises by assembly participants, such as hoods or masks, or taking other steps to participate anonymously may form part of the expressive element of a peaceful assembly or serve to counter reprisals or to protect privacy, including in the context of new surveillance technologies. […]

61. While the collection of relevant information and data by authorities may under certain circumstances assist the facilitation of assemblies, it must not result in suppressing rights or creating a chilling effect. Any information gathering, whether by public or private entities, including through surveillance or the interception of communications, and the way in which data are collected, shared, retained and accessed, must strictly conform to applicable international standards, including on the right to privacy, and may never be aimed at intimidating or harassing participants or would-be participants in assemblies. […]

62. The mere fact that a particular assembly takes place in public does not mean that participants' privacy cannot be violated. The right to privacy may be infringed, for example, by facial recognition and other technologies that can identify individual participants in a crowd. The same applies to the monitoring of social media to glean information about participation in peaceful assemblies. Independent and transparent scrutiny and oversight must be exercised over the decision to collect the personal information and data of those engaged in peaceful assemblies and over its sharing or retention, with a view to ensuring the compatibility of such actions with the Covenant.

94. The use of recording devices by law enforcement officials during assemblies, including body-worn cameras, may play a positive role in securing accountability, if used judiciously. However,

the authorities should have clear and publicly available guidelines to ensure that their use is consistent with international standards on privacy and does not have a chilling effect on participation in assemblies. Participants, journalists and monitors also have the right to record law enforcement officials.

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

43. Systematic surveillance of people in the public space online and offline, in particular when combined with additional ways to analyse and connect the obtained information with other data sources, constitutes an interference with the right to privacy and can have highly detrimental effects on the enjoyment of other human rights. It may constitute a threat to freedom of expression and peaceful assembly, participation and democracy and should therefore be approached with utmost caution and only in strict adherence with human rights requirements. This is the case even though the activities monitored are occurring in public, or on open social media platforms, as individuals should have a space free from systematic observation and intrusion, in particular by government entities. […] the protection of the right to privacy extends to public spaces and information that is publicly available. […]

47. […] surveillance has considerable chilling effects on how people exercise their rights, in particular the right to freedom of expression and peaceful assembly. […]

Report of the United Nations High Commissioner for Human Rights, Promotion and Protection of the Human Rights and Fundamental Freedoms of Africans and of People of African Descent Against Excessive Use of Force and Other Human Rights Violations by Law Enforcement Officers, UN Doc A/HRC/47/53 (1 June 2021)

47. […] The use of surveillance tools and other technologies to monitor protests and of COVID-19 measures to restrict them were also highlighted as a concern in some instances. […]

Report of the Working Group on Enforced and Involuntary Disappearances, 'New technologies and enforced disappearances', UN Doc A/HRC/54/22/Add.5 (11 September 2023)

65. […] the Working Group recommends that States: (j) Ensure that individuals or civil society organizations targeted can exercise their right to an effective remedy and obtain reparation;

Report of the Special Rapporteur on the Promotion and Protection of Human Rights while Counter-Terrorism, Human Rights Implications of the Development, Use, Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism, UN Doc A/HRC/52/39 (1 March 2023)

34. She is additionally deeply concerned about the use of drones to surveil protests. She underscores again that this is consistent with the broader trend she identifies of the short-lived exceptional use of certain technologies and their rapid reinvention as ordinary State practice. In addition to the obvious implications for privacy, freedom of assembly, freedom of expression and the right to participate in political affairs, the use of drones coupled with the coercive power of the police brings the issues of arbitrary detention, the liberty and security of the person, and the right to life into play.

56. The Special Rapporteur recommends that States: (f) Provide adequate and accessible remedies to individuals whose personal information has been mishandled or misused in counter-terrorism or preventing and countering violent extremism concerns;

Interim report of the Special Rapporteur on Freedom of Religion or Belief, 'Indigenous peoples and the right to freedom of religion or belief', UN Doc A/77/514 (10 October 2022)

68. In both violating indigenous peoples' rights and limiting their advocacy against such violations, several States allegedly have intimidated, surveilled, threatened, arbitrarily arrested or violently attacked peaceful indigenous protestors with excessive force. […]

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and Association, 'Protection of human rights in the context of peaceful protests during crisis situations', UN Doc A/HRC/50/42 (16 May 2022)

58. States have employed various new technologies during protests in the context of crises, including surveillance technologies such as CCTV cameras, body cameras and aerial surveillance vehicles, and face recognition technology. Surveillance technologies have frequently been deployed without transparency and accountability, and have been used to crack down on peaceful protests. The use of surveillance technology has expanded dramatically during the COVID-19 pandemic, in a manner that has serious implications for State monitoring and suppressing of protests and dissent. […] [Camera surveillance] must be used in a transparent manner, according to strict legal safeguards and in accordance with privacy laws complying with human rights standards. Authorities have also engaged in online surveillance with particular intensity in times of crisis, often resulting in arrests and charges under overly broad and vague laws penalizing "fake news", "attacking the image of the State", incitement and other purported crimes.

78. In regard to respecting and enabling peaceful protest during crisis situations, States should: (m) Refrain from the use of biometric identification and recognition technologies, such as facial recognition, for arbitrary surveillance of protesters, both offline and online;

Report of the Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, The Guiding Principles on Business and Human Rights: Guidance on Ensuring Respect for Human Rights Defenders, UN Doc A/HRC/47/39/Add.2 (22 June 2021)

104. States, business enterprises, and development finance institutions investing in and/or implementing development projects, may find themselves linked to, or complicit in human rights abuses targeting defenders due to engaging in, or reacting to, conflicts that target human rights defenders. For example, in order to facilitate business access to an area, or the advancement of a project. In other contexts, they may be involved in shutting down protests, conducting surveillance on defenders, or restricting trade union activity.

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, Access to Justice as an Integral Element of the Protection of Rights to Freedom of Peaceful Assembly and Association, UN Doc A/HRC/47/24 (12 May 2021)

50. The Special Rapporteur notes that in some countries identity controls and confiscation of objects are practised in a discriminatory manner before protests, and there is often no effective remedy against them. The use of such identity controls amounts to a type of profiling and surveillance that has a potentially chilling effect on the right to freedom of peaceful assembly. Any alleged cases of abuse of power or of misconduct by law enforcement that is motivated by racial or other discrimination during preventive identity controls in the context of protests should be investigated effectively. […]

57. The Special Rapporteur has also received information regarding the abuse of technologies, such as facial recognition tools, and the surveillance of social media sites used by activists, of phone recordings and of location tracking from around the world. States should refrain from conducting targeted surveillance using digital tools against protesters. He believes that certain practices,

whereby the protection from violation of the right to privacy can be raised in criminal proceedings by claiming unlawfulness of such evidence, are promising. One such example is when the technical means used to get the information were not proportional, e.g., in Slovakia. Yet, he supports the call to impose an immediate moratorium on privately developed surveillance technologies to be lifted until a human rights-compliant regime has been established.

60. Similarly, the lawyers who were interviewed noticed that they had been denied access to full files and documentation, such as footage obtained by the authorities during protests. As mentioned above, surveillance tools have been used to monitor lawful protests, but they have also been used in some contexts while in police custody, in particular to intercept communications between persons deprived of their liberty and their lawyers, e.g., in China; France; Hong Kong, China; Hungary; Kenya; Spain; and Poland.

69. The Special Rapporteur notes with concern that a majority of the lawyers and legal practitioners interviewed had faced threats and harassment and, in some contexts, even criminalization. The Special Rapporteur has received information regarding surveillance, confiscation of confidential documents, raids of offices, detention and disbarment of lawyers working for the promotion and protection of freedom of peaceful assembly and of association in many countries.

70. The Special Rapporteur has voiced his concern regarding the indiscriminate surveillance of those exercising their right of peaceful assembly, but intrusive online surveillance is also used to monitor or interfere with lawyer-client communications. This practice has considerable negative impacts on access to justice, as well as on the rights to freedom of peaceful assembly and of association. When someone exercising their right to freedom of peaceful assembly or of association is detained or is in police custody, the likelihood of surveillance from the authorities increases. Authorities must ensure the confidentiality of all communications between lawyers and their clients; if needed, technical solutions to secure and protect them, including measures for encryption and anonymity, must be allowed."

74. In order to comply with their human rights obligations and ensure access to justice in the context of the rights to freedom of peaceful assembly and of association, the Special Rapporteur recommends that States: (l) Establish independent mechanisms to monitor and investigate the use of digital technologies for surveillance in the context of the rights to freedom of peaceful assembly and of association, with a view to ensuring that any such use is consistent with the principles of legality, necessity and legitimacy of objective.

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association – Ten Years Protecting Civic Space Worldwide, UN Doc A/HRC/44/50 (13 May 2020)

24. In a report to the Council, the Special Rapporteur examined how Governments were increasingly imposing limitations in the exercise of the rights to freedom of peaceful assembly and of association. Drawing on seven years of communications and thematic reports, the report mapped the myriad of legal and extralegal measures being adopted around the world, including the adoption of national security, counter-terrorism and public order laws; the criminalization of peaceful protest; the indiscriminate and excessive use of force to counter or repress peaceful protest; the stigmatization of and attacks against civil society actors; and censorship and surveillance of the digital space.

68. Technological advances such as facial recognition, artificial intelligence, hacking tools and digital identification, are posing complex challenges to association and assembly rights. Governments are increasingly cutting off access to the Internet and mobile networks to stifle mass demonstrations and silent dissident voices during elections. For many in civil society, the Internet is no longer a safe place, as they have become the growing targets of surveillance and online violence. The slow progress in addressing these challenges points to the urgent need to move beyond commitments to action and accountability.

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, UN Doc A/74/349 (11 September 2019)

44. […] The Special Rapporteur has affirmed that stopping individuals at random, with no specific evidence that they had committed or were about to commit a crime, requesting identification and detaining them if identification cannot be produced, amounts to a type of profiling and surveillance that has the potential to "chill" the exercise of the right to freedom of peaceful assembly and disproportionately affects groups at risk, including people living in poverty. Poor communities are also more likely to experience violations of privacy and intrusion on their homes in the context of protests than their well-off neighbours. […]

Report of the Special Rapporteur on Freedom of Religion or Belief, UN Doc A/HRC/40/58 (5 March 2019)

11. […] The Special Rapporteur wishes to raise concern about the many reports he has received detailing surveillance, intimidation, harassment, prosecution, threats of bodily harm, torture or murder following acts that had exceeded the limits imposed by law or social convention on peaceful manifestations of thoughts, conscience, and religion or belief, and/or that had offended the sensitivities of others by denigrating what they held sacred.

Concluding Observations on the Second Periodic Report of Indonesia, Human Rights Committee, UN Doc CCPR/C/IDN/CO/2, (26 March 2024)

37. In accordance with article 21 of the Covenant and the Committee's general comment No. 37 (2020) on the right of peaceful assembly, the State party should: […] (c) Ensure that all allegations of harassment, intimidation, surveillance and excessive use of force are investigated promptly, thoroughly and impartially, that those found responsible are prosecuted and, if found guilty, punished and that victims are afforded effective remedies;

Concluding Observations on the Eighth Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/8 (26 March 2024)

53. […] [T]he State party should end the use of facial recognition and other mass surveillance technologies by law enforcement agencies at protests, in order to safeguard privacy, non-discrimination, freedom of expression and association and assembly rights for protesters.

Concluding Observations on the Sixth Periodic Report of Sri Lanka, Human Rights Committee, UN Doc CCPR/C/LKA/CO/6 (21 March 2023)

43. The State party should: (c) Ensure that allegations of excessive use of force during peaceful assemblies and of harassment, violence and surveillance of members of civil society are investigated promptly, thoroughly and impartially, that those allegedly responsible are prosecuted and, if found guilty, punished and that the victims obtain redress;

Concluding Observations on the Eighth Periodic Report of the Russian Federation, Human Rights Committee, UN Doc CCPR/C/RUS/CO/8 (1 November 2022)

32. […] It is concerned about reports that participation in assemblies is hampered by the use of preventive detention and by the use of facial recognition systems that are not regulated by law, including in regard to the procedure for storing and reviewing data relating to such systems (arts. 7, 9–10, 14, 17, 19 and 21).

33. In accordance with article 21 of the Covenant and in the light of the Committee's general

comment No. 37 (2020) on the right of peaceful assembly, the State party should: (e) Refrain from the use of facial recognition systems and the practice of preventive detention to hamper participation in peaceful assemblies.

Concluding Observations on the Fifth Periodic Report of the Netherlands, Human Rights Committee, UN Doc CCPR/C/NLD/CO/5 (22 August 2019)

60. The Committee is concerned that the provisions of the Public Assemblies Act, including the provision that allows mayors to end and prohibit an assembly in the absence of prior notification, are not consistent with the Covenant. It is also concerned about the increasing degree of police surveillance and the use of identity checks during peaceful demonstrations, which reportedly have a chilling effect on demonstrators (art. 21).

Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee, UN Doc CCPR/C/POL/CO/7 (4 November 2016)

39. […] The Committee is particularly concerned about: e) the possibility of banning or terminating assemblies and mass events;

Committee on the Rights of the Child, General Comment No 25 (2021) on Children's Rights in Relation to the Digital Environment, UN Doc CRC/C/GC/25 (2 March 2021)

65. States parties should ensure that their laws, regulations and policies protect children's right to participate in organizations that operate partially or exclusively in the digital environment. No restrictions may be placed on the exercise by children of their right to freedom of association and peaceful assembly in the digital environment other than those that are lawful, necessary and proportionate. Such participation should be safe, private and free from surveillance by public or private entities.

Committee on the Elimination of Racial Discrimination, General Recommendation No 36 (2020) on Preventing and Combating Racial Profiling by Law Enforcement Officials, UN Doc CERD/C/GC/36 (17 December 2020)

35. The increasing use of facial recognition and surveillance technologies to track and control specific demographic groups raises concerns with respect to many human rights, including the right to privacy, freedom of peaceful assembly and association, freedom of expression and freedom of movement. It is designed to automatically identify individuals based on their facial geometry, potentially profiling people based on grounds of discrimination such as race, colour, national or ethnic origin or gender. Cameras equipped with real-time facial recognition technology are widely applied for the purpose of flagging and tracking of individuals, which may enable Governments and others to keep records of the movements of large numbers of individuals, possibly based on protected characteristics. Moreover, it has been demonstrated that the accuracy of facial recognition technology may differ depending on the colour, ethnicity or gender of the persons assessed, which may lead to discrimination.

***Catt v The United Kingdom*, App No 43514/15, Judgment, European Court of Human Rights (24 January 2019)**

94. As the Court has recalled the expression "in accordance with the law" not only requires the impugned measure to have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope and discretion conferred on the competent authorities and the manner of its exercise.

97. In light of the general nature of the police powers and the variety of definitions of the term "domestic extremism", the Court considers that there was significant ambiguity over the criteria being used by the police to govern the collection of the data in question. […] The Court therefore agrees with the applicant that from the information available it is difficult to determine the exact scope and content of the data being collected and compiled to form the database.

98. […] The Court notes that the existence of a specific database was not clearly acknowledged until the domestic proceedings in this case, although it accepts that from the information publicly available it was possible to deduce that the police were likely to be maintaining such a database.

99. It is of concern that the collection of data for the purposes of the database did not have a clearer and more coherent legal base. However, the framework governing the collection of the applicant's data cannot be viewed in isolation from the provisions governing retention and use of the applicant's personal data. […]

105. The Court has concerns about the ambiguity of the legal basis for the collection of the applicant's personal data. In particular the Court notes the loosely defined notion of "domestic extremism" and the fact that applicant's data could potentially be retained indefinitely. However, the data retained would not be disclosed to third parties; and the applicant had the possibility to apply for the deletion of his data.

112. However, the Court considers in the present case there are reasons for doing so. In the first place it considers significant that personal data revealing political opinion falls among the special categories of sensitive data attracting a heightened level of protection […].

114. The Court also recalls the importance of examining compliance with the principles of Article 8 where the powers vested in the state are obscure, creating a risk of arbitrariness especially where the technology available is continually becoming more sophisticated […].

123. Moreover, the absence of effective safeguards was of particular concern in the present case, as personal data revealing political opinions attracts a heightened level of protection. Engaging in peaceful protest has specific protection under Article 11 of the Convention, which also contains special protection for trade unions, whose events the applicant attended. In this connection it notes that in the National Coordinator's statement, the definition of "domestic extremism" refers to collection of data on groups and individuals who act "outside the democratic process". Therefore, the police do not appear to have respected their own definition (fluid as it may have been (see paragraph 105)) in retaining data on the applicant's association with peaceful, political events: such events are a vital part of the democratic process. The Court has already highlighted the danger of an ambiguous approach to the scope of data collection in the present case. Accordingly, it considers that the decisions to retain the applicant's personal data did not take into account the heightened level of protection it attracted as data revealing a political opinion, and that in the circumstances its retention must have had a "chilling effect".

Annual Report of the Inter-American Commission on Human Rights 2019, Volume II – Annual Report of the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II. Doc 5 (24 February 2020)

Protest and Human Rights – Standards on the Rights Involved in Social Protest and the Obligations to Guide the Response of the State

236. These practices [of illegal espionage] often include filming and/or photographing demonstrators, resulting in data registries on individuals or organizations. Their telephone conversations or their private communications through digital media may also be monitored. Cases in which these clandestine records are used to produce documents, files, and databases in intelligence, security, and justice institutions that stigmatize political parties, organizations, and social movements are

particularly serious. This kind of information has even become part of judicial proceedings in cases that criminalize demonstrators and social leaders.

301. In no case can mere participation in protests, or in their announcement or organization, justify the violation of the right to privacy with respect to private communications made by a person, whether in writing, by voice or images, and regardless of the platform used. The right to privacy encompasses not only individual communications, but also communications that take place in closed groups to which only members have access.

302. There have been reports in the region of police and military officers infiltrating social networks or using false identities in order to obtain information about social movements and the organization of demonstrations and protests. Such a practice may be considered a serious violation of the rights of assembly and freedom of association, and even of the right to privacy. Under no circumstances are online intelligence actions allowed to monitor people who organize or take part in social protests.

347. Individuals, groups, and social or political movements participating in demonstrations and protests must be protected from undue interference in their right to privacy.

SECTION 4: SURVEILLANCE AND OTHER HUMAN RIGHTS PROVISIONS

A. SURVEILLANCE AND THE JURISDICTIONAL CLAUSE (EXTRATERRITORIAL APPLICATION)

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

Emphasizing that unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data, hacking and the unlawful use of biometric technologies, as highly intrusive acts, violate the right to privacy, […] including when undertaken extraterritorially or on a mass scale,

Deeply concerned at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights,

**See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014)*

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

9. A State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State party, even if not situated within its territory. Human rights law applies where a State exercises its power or effective control in relation to digital communications infrastructure, wherever located, for example through direct tapping or penetration of communications infrastructure located outside the territory of that State. Equally, where a State exercises regulatory jurisdiction over a third party that controls a person's information (for example, a cloud service provider), that State also has to extend human rights protections to those whose privacy would be affected by accessing or using that information.

36. In terms of its scope, the legal framework for surveillance should cover State requests to business enterprises. It should also cover access to information held extraterritorially or information-sharing with other States. A structure to ensure accountability and transparency within governmental organizations carrying out surveillance needs to be clearly established in the law.

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

34. […] [Digital surveillance] may engage a State's human rights obligations if that surveillance the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obligations under the Covenant. If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation of those companies in that country then human rights protections must be extended

those whose privacy is being interfered with, whether in the country of incorporation or beyond. This holds whether or not such an exercise of jurisdiction is lawful in the first place, or in fact violated another State's sovereignty.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

56. At the same time, targeted surveillance is not always territorially contained. When States reach beyond their borders to conduct targeted surveillance, it may be difficult for the individuals targeted by such surveillance to bring claims against the offending State. Some of the same evidentiary and other burdens as in domestic claims may be present in these cases as well. Moreover, as in the *Doe* case noted above, courts may be unwilling to entertain lawsuits against foreign sovereigns. While the rules for such suits vary, States should interpret the norms of sovereign immunity to ensure that their courts may entertain suits against foreign Governments.

Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, UN Doc CCPR/C/ITA/CO/6 (28 March 2017)

37. The State Party should […] take measures to ensure that all corporations under its jurisdiction, in particular technology corporations, respect human rights standards when engaging in operations abroad.

Concluding Observations on the Fifth Periodic Report of France, Human Rights Committee, UN Doc CCPR/C/FRA/CO/5 (17 August 2015)

12. […] The State Party should take all necessary steps to guarantee that its surveillance activities within and outside its territory are in conformity with its obligations under the Covenant, in particular, Article 17.

***Wieder and Guarnieri v the United Kingdom*, Apps Nos 64371/16 and 64407/16, Judgment, European Court of Human Rights (12 September 2023)**

89. The applicants in the present case have not suggested that they were themselves at any relevant time in the United Kingdom or in an area over which the United Kingdom exercised effective control. Rather, they contend either that the acts complained of – being the interception, extraction, filtering, storage, analysis and dissemination of their communications by the United Kingdom intelligence agencies pursuant to the section 8(4) regime (see paragraph 56 above) – nevertheless fell within the respondent Government's territorial jurisdiction, or, in the alternative, that one of the exceptions to the principle of territoriality applied.

90. In *Big Brother Watch and Others* the Court identified four stages to the bulk interception process: the interception and initial retention of communications and related communications data; the searching of the retained communications and related communications data through the application of specific selectors; the examination of selected communications/related communications data by analysts; and the subsequent retention of data and use of the "final product", including the sharing of data with third parties (ibid, § 325). Although it did not consider that the interception and initial retention constituted a particularly significant interference, in its view the degree of interference with individuals' Article 8 rights increased as the bulk interception process progressed (ibid, § 330). The principal interference with the Article 8 rights of the sender or recipient was therefore the searching, examination and use of the intercepted communications.

91. In the context of the section 8(4) regime each of the steps which constituted an interference with the privacy of electronic communications, being the interception and, more particularly, the

searching, examining and subsequent use of those intercepted communications, were carried out by the United Kingdom intelligence agencies acting – to the best of the Court's knowledge - within United Kingdom territory.

92. It is the Government's contention that any interference with the applicants' private lives occasioned by the interception, storage, searching and examination of their electronic communications could not be separated from their person and would therefore have produced effects only where they themselves were located – that is, outside the territory of the United Kingdom (see paragraph 77 above).

93. However, such an approach is not supported by the case-law of the Court. Although there are important differences between electronic communications, for the purposes of Article 8 of the Convention, and possessions, for the purposes of Article 1 of Protocol No. 1, it is nevertheless the case that an interference with an individual's possessions occurs where the possession is interfered with, rather than where the owner is located (see, for example, Anheuser-Busch Inc. v. Portugal [GC], no. 73049/01, ECHR 2007-I). Similarly, in the specific context of Article 8, it could not seriously be suggested that the search of a person's home within a Contracting State would fall outside that State's territorial jurisdiction if the person was abroad when the search took place. While some of the elements of a person's private life (for example, physical integrity) may not readily be separated from his or her physical person, that is not necessarily the case for all such elements. For example, in Von Hannover v. Germany (no. 59320/00, ECHR 2004-VI) the Court appeared to accept that the interference with the applicant's private life which flowed from the publication by German magazines of photographs of her took place in Germany, where the photographs had been published and viewed by the magazines' readership (ibid., §§ 53 and 76-81), even though the applicant lived in France and had her official residence in Monaco (, § 8), and the photographs in question had been taken in Austria, France and Monaco (ibid., §§ 11-17). Similarly, in Arlewin v. Sweden (no. 22302/10, §§63 and 65, 1 March 2016) the Court found that injury to the applicant's privacy and reputation occasioned by the broadcast of a television programme took place in Sweden, where the programme was broadcast, and not in the United Kingdom, where the broadcaster had its head office.

94. Turning to the facts of the case at hand, the interception of communications and the subsequent searching, examination and use of those communications interferes both with the privacy of the sender and/or recipient, and with the privacy of the communications themselves. Under the section 8(4) regime the interference with the privacy of communications clearly takes place where those communications are intercepted, searched, examined and used and the resulting injury to the privacy rights of the sender and/or recipient will also take place there.

95. Accordingly, the Court considers that the interference with the applicants' rights under Article 8 of the Convention took place within the United Kingdom and therefore fell within the territorial jurisdiction of the respondent State. As such, it is not necessary to consider whether any of the exceptions to the territoriality principle are applicable.

UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/51/9 (6 October 2022)*

Equally concerned about incidents of the extraterritorial targeting of journalists and media workers, including killings, enforced disappearances, harassment and surveillance,

2. *Also condemns unequivocally* the extraterritorial targeting of journalists and media workers, including killings, enforced disappearances, harassment and surveillance, and urges States to cease and/or refrain from such attacks or measures;

** UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/45/18 (12 October 2020)*

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014)

62. The Special Rapporteur concurs with the High Commissioner for Human rights that where States penetrate infrastructure located outside their territorial jurisdiction, they remain bound by their obligations under the Covenant.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/23/40 (17 April 2013)

76. […] States should exercise adequate oversight in order to meet their international human rights obligations when they contract with, or legislate for, corporate actors where there may be an impact upon the enjoyment of human rights. Human rights obligations in this regard apply when corporate actors are operating abroad.

Concluding Observations on the Fifth Periodic Report of the United States of America, Human Rights Committee, UN Doc CCPR/C/USA/CO/5 (30 October 2023)

57. […] the State party should ensure that its surveillance activities, both within and outside its territory, conform to its obligations under the Covenant, under article 17, and that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under surveillance. […]

Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee, UN Doc CCPR/C/POL/CO/7 (4 November 2016)

39. The Committee is concerned about the surveillance and interception powers of the Polish intelligence and law enforcement authorities as reflected in the Law on Counterterrorism of June 2016 and the Act amending the Police Act and certain other acts of January 2016. The Committee is particularly concerned about: (b) the targeting of foreign nationals and application of different legal criteria to them.

Concluding Observations on the Sixth Periodic Report of New Zealand, Human Rights Committee, UN Doc CCPR/C/NZL/CO/6 (28 April 2016)

15. The Committee is further concerned about the limited judicial authorization process for the interception of communications of New Zealanders and the total absence of such authorization for the interception of communications of non-New Zealanders.

16. The State party should take all appropriate measures to ensure that: ...(b) Sufficient judicial safeguards are implemented, regardless of the nationality or location of affected persons, in terms of interception of communications and metadata collection, processing and sharing.

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/7 (17 August 2015) *

24. […] measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance.

**See also Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, UN Doc CCPR/C/USA/CO/4 (23 April 2014), para. 22*

***Big Brother Watch and Others v The United Kingdom*, Apps Nos 58170/13, 62322/14 and 24960/15, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

495. In the Chamber's view, the interception of communications by foreign intelligence services could not engage the responsibility of a receiving State, or fall within that State's jurisdiction within the meaning of Article 1 of the Convention, even if the interception was carried out at that State's request (see paragraph 420 of the Chamber judgment). […] the interception of communications by a foreign intelligence service could only fall within the receiving State's jurisdiction if that State was exercising authority or control over the foreign intelligence service […].

496. […] Therefore, any interference with Article 8 of the Convention could only lie in the initial request and the subsequent receipt of intercept material, followed by its subsequent storage, examination and use by the intelligence services of the receiving State.

497. The protection afforded by the Convention would be rendered nugatory if States could circumvent their Convention obligations by requesting either the interception of communications by, or the conveyance of intercepted communications from, non-Contracting States; or even, although not directly in issue in the cases at hand, by obtaining such communications through direct access to those States' databases. Therefore, in the Court's view, where a request is made to a non-contracting State for intercept material the request must have a basis in domestic law, and that law must be accessible to the person concerned and foreseeable as to its […]. It will also be necessary to have clear detailed rules which give citizens an adequate indication of the circumstances in which and the conditions on which the authorities are empowered to make such a request […] and which provide effective guarantees against the use of this power to circumvent domestic law and/or the States' obligations under the Convention.

498. Upon receipt of the intercept material, the Court considers that the receiving State must have in place adequate safeguards for its examination, use and storage; for its onward transmission; and for its erasure and destruction. These safeguards, first developed by the Court in its case-law on the interception of communications by Contracting States, are equally applicable to the receipt, by a Contracting State, of solicited intercept material from a foreign intelligence service. If, as the Government contend, States do not always know whether material received from foreign intelligence services is the product of interception, then the Court considers that the same standards should apply to all material received from foreign intelligence services that could be the product of intercept.

499. Finally, the Court considers that any regime permitting the intelligence services to request either interception or intercept material from non-Contracting States, or to directly access such material, should be subject to independent supervision, and there should also be the possibility for independent *ex post facto* review.

***Weber and Saravia v Germany*, App No 54934/00, Decision, European Court of Human Rights (29 June 2006)**

87. The Court reiterates that the term "law" within the meaning of the Convention refers back to national law, including rules of public international law applicable in the State concerned. As regards allegations that a respondent State has violated international law by breaching the territorial sovereignty of a foreign State, the Court requires proof in the form of concordant inferences that the authorities of the respondent State have acted extraterritorially in a manner that is inconsistent with

the sovereignty of the foreign State and therefore contrary to international law.

88. The Court observes that the impugned provisions of the amended G10 Act authorise the monitoring of international wireless telecommunications, that is, telecommunications which are not effected via fixed telephone lines but, for example, via satellite or radio relay links, and the use of data thus obtained. Signals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany. In the light of this, the Court finds that the applicants failed to provide proof in the form of concordant inferences that the German authorities, by enacting and applying strategic monitoring measures, have acted in a manner which interfered with the territorial sovereignty of foreign States are protected in public intentional law.

***Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems* (C-311/18), Judgment, Grand Chamber, Court of Justice of the European Union (16 July 2020)**

180. It is thus apparent that Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes. In those circumstances and as the Advocate General stated, in essence, in points 291, 292 and 297 of his Opinion, that article cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter, as interpreted by the case-law set out in paragraphs 175 and 176 above, according to which a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards.

B. SURVEILLANCE AND THE PRINCIPLE OF NON-DISCRIMINATION

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

Noting also that violations and abuses of the right to privacy in the digital age can affect all individuals, with particular effects on women, children, persons with disabilities and older persons, as well as persons in vulnerable situations and marginalized groups, and that the processing of personal data must be subject to human rights safeguards and restrictions, especially the data of persons in vulnerable situations,

Noting with concern also that certain predictive algorithms and the increasing use of facial recognition and surveillance technologies are likely to result in discrimination, in particular when data used in the training of algorithms are not accurate, relevant and representative and audited against encoded bias,

Noting that the use of artificial intelligence may, without human rights safeguards, pose the risk of reinforcing discrimination, including structural inequalities, especially when processing sensitive data, and recognizing that racially and otherwise discriminatory outcomes must be prevented in the conception, design, development, deployment and use of new and emerging digital technologies,

Noting with concern reports indicating lower accuracy of biometric data identification, including facial recognition technologies that show racial identification biases and prejudices against women, including when non-representative training data are used, and that the use of digital technologies can reproduce, reinforce and even exacerbate racial and gender inequalities, and recognizing in this context the importance of effective remedies,

10. *Calls upon* all States: (l) To develop, review, implement and strengthen gender-responsive policies and programmes that contribute to the empowerment of all women and girls and promote and protect the right of all individuals to privacy in the digital age;

** See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/34/7 (23 March 2017)*

UN Human Rights Council Resolution on New and Emerging Digital Technologies and Human Rights, UN Doc A/HRC/RES/53/29 (14 July 2023)

Recognizing further that the risks that new and emerging digital technologies have for the protection, promotion and enjoyment of human rights can affect women and girls disproportionately, including by perpetuating existing patterns of gender inequality and discrimination, further exacerbated by the underrepresentation of women in the sectors of science, technology, engineering and maths, limiting their involvement in the design and development of new technologies, and stressing the need to address violence against women and girls, including sexual and gender-based violence, that occurs through or is amplified by the use of technology, […]

3. *Highlights* the importance of the need to respect, protect and promote human rights and fundamental freedoms, in recognition of the inherent dignity of the human person, throughout the lifecycle of artificial intelligence systems and, towards this end, the need to pay particular attention to: […] (b) Protecting individuals from discrimination on the basis of, inter alia, race, gender, age, disability, nationality, religion and language resulting from the conception, design, use, deployment and further deployment of artificial intelligence systems, while paying attention to individuals at greater risk of having their rights disproportionately affected by artificial intelligence, including persons belonging to national or ethnic, religious, linguistic or racial minorities, Indigenous Peoples as well as local communities, persons in rural areas, economically disadvantaged persons and persons in vulnerable or marginalized situations, including by ensuring that data used in the training of algorithms are accurate, relevant and representative and audited against encoded bias;

Report of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/48/31 (13 September 2021)

26. Remote real-time biometric recognition raises serious concerns under international human rights law, which the High Commissioner has highlighted previously. Some of these concerns reflect the problems associated with predictive tools, including the possibility of erroneous identification of individuals and disproportionate impacts on members of certain groups. Moreover, facial recognition technology can be used to profile individuals on the basis of their ethnicity, race, national origin, gender and other characteristics.

Report of the United Nations High Commissioner for Human Rights on the Promotion and Protection of the Human Rights and Fundamental Freedoms of Africans and of People of African Descent Against Excessive Use of Force and Other Human Rights Violations by Law Enforcement Officers, UN Doc A/HRC/47/53 (1 June 2021)

25. […] Concerns have also been reported in relation to the application of algorithmic decision-making and artificial intelligence such as the use of facial recognition and surveillance technologies to track and control specific demographic groups, in predictive policing and in risk assessments linked to sentencing. […]

47. […] The use of surveillance tools and other technologies to monitor protests and of COVID-19 measures to restrict them were also highlighted as a concern in some instances. […]

48. […] In Europe and the United States, some civil society activists of African descent reported harassment, surveillance, threats to their safety, including online, stigmatization and other forms of pressure. […]

50. […] It is critical that States honour their obligations to protect those standing up against racism, including human rights defenders, from being discredited, harassed, intimidated and subjected to increased surveillance, both within and outside the context of assemblies.

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

35. [there exist] ongoing discussions on whether "foreigners" and "citizens" should have equal access to privacy protections within national security surveillance oversight regimes. Several legal regimes distinguish between the obligations owed to nationals or those within a State's territories, and non-nationals and those outside, or otherwise provide foreign or external communications with lower levels of protection. If there is uncertainty around whether data are foreign or domestic, intelligence agencies will often treat the data as foreign (since digital communications regularly pass "off-shore" at some point) and thus allow them to be collected and retained. The result is significantly weaker – or even non-existent – privacy protection for foreigners and non-citizens, as compared with those of citizens.

36. International human rights law is explicit with regard to the principle of non-discrimination. Article 26 of the International Covenant on Civil and Political Rights provides that "all persons are equal before the law and are entitled without any discrimination to the equal protection of the law" and, further, that "in this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." These provisions are to be read together with articles 17, which provides that "no one shall be subjected to arbitrary interference with his privacy" and that "everyone has the right to the protection of the law against such interference or attacks", as well as with article 2, paragraph 1. [...]

Committee on the Elimination of Racial Discrimination, General Recommendation No 36 (2020) on Preventing and Combating Racial Profiling by Law Enforcement Officials, UN Doc CERD/C/GC/36 (17 December 2020)

35. The increasing use of facial recognition and surveillance technologies to track and control specific demographic groups raises concerns with respect to many human rights, including the right to privacy, freedom of peaceful assembly and association, freedom of expression and freedom of movement. It is designed to automatically identify individuals based on their facial geometry, potentially profiling people based on grounds of discrimination such as race, colour, national or ethnic origin or gender. Cameras equipped with real-time facial recognition technology are widely applied for the purpose of flagging and tracking of individuals, which may enable Governments and others to keep records of the movements of large numbers of individuals, possibly based on protected characteristics. Moreover, it has been demonstrated that the accuracy of facial recognition technology may differ depending on the colour, ethnicity or gender of the persons assessed, which may lead to discrimination.

38. As a prerequisite, and without prejudice to further measures, comprehensive legislation against racial discrimination, including civil and administrative law as well as criminal law, is

indispensable to combating racial profiling effectively. […]

58. States should ensure that algorithmic profiling systems used for the purposes of law enforcement are in full compliance with international human rights law. To that effect, before procuring or deploying such systems States should adopt appropriate legislative, administrative and other measures to determine the purpose of their use and to regulate as accurately as possible the parameters and guarantees that prevent breaches of human rights. Such measures should, in particular, be aimed at ensuring that the deployment of algorithmic profiling systems does not undermine the right not to be discriminated against, the right to equality before the law, the right to liberty and security of person, the right to the presumption of innocence, the right to life, the right to privacy, freedom of movement, freedom of peaceful assembly and association, protections against arbitrary arrest and other interventions, and the right to an effective remedy.

61. States should take all appropriate measures to ensure transparency in the use of algorithmic profiling systems. This includes public disclosure of the use of such systems and meaningful explanations of the ways in which the systems work, the data sets that are being used, and the measures in place to prevent or mitigate human rights harms.

62. States should adopt measures to ensure that independent oversight bodies have a mandate to monitor the use of artificial intelligence tools by the public sector, and to assess them against criteria developed in conformity with the Convention to ensure they are not entrenching inequalities or producing discriminatory results. States should also ensure that the functioning of such systems is regularly monitored and evaluated in order to assess deficiencies and to take the necessary corrective measures. When the results of an assessment of a technology indicate a high risk of discrimination or other human rights violations, States should take measures to avoid the use of such a technology.

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/7, para. 24 (17 August 2015)*

[…] measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance.

**See also Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, UN Doc CCPR/C/USA/CO/4, para. 22 (23 April 2014)*

Committee on the Rights of the Child, General Comment No 25 (2021) on Children's Rights in Relation to the Digital Environment, UN Doc CRC/C/GC/25 (2 March 2021)

103. […] Standards for digital educational technologies should ensure that the use of those technologies is ethical and appropriate for educational purposes and does not expose children to violence, discrimination, misuse of their personal data, commercial exploitation or other infringements of their rights, such as the use of digital technologies to document a child's activity and share it with parents or caregivers without the child's knowledge or consent.

***Draft Agreement between Canada and the European Union on the Transfer of Passenger Name Record data* (1/15), Court of Justice of the European Union, Grand Chamber, Opinion pursuant to Article 218(11) TFEU (26 July 2017)**

174. Lastly, in order to ensure that, in practice, the pre-established models and criteria, the use that is made of them and the databases used are not discriminatory and are limited to that which is strictly necessary, the reliability and topicality of those pre-established models and criteria and

databases used should, taking account of statistical data and results of international research, be covered by the joint review of the implementation of the envisaged agreement […]

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

Noting also that violations and abuses of the right to privacy in the digital age can affect all individuals, with particular effects on women, children, in particular girls, persons with disabilities and older persons, as well as those in vulnerable situations, […]

Noting that the use of artificial intelligence may, without proper technical, regulatory, legal and ethical safeguards, pose the risk of reinforcing discrimination, including structural inequalities, and recognizing that racially and otherwise discriminatory outcomes should be prevented in the design, development, implementation and use of emerging digital technologies,

Noting with concern reports indicating lower accuracy of facial recognition technologies with certain groups, including when non-representative training data are used, that the use of digital technologies can exacerbate racial inequality and in this context the importance of effective remedies,

** See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016)*

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019)*

Noting with concern that automatic processing of personal data for individual profiling, automated decision-making and machine learning technologies may, without adequate safeguards, lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights, and recognizing the need to apply international human rights law in the design, development, evaluation and regulation of these technologies, and to ensure they are subject to adequate safeguards and oversight,

** See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/34/7 (23 March 2017)*

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

46. Surveillance operations tend to disproportionately target minorities and marginalized communities. The use of artificial intelligence risks perpetuating such patterns of discrimination, including the use of facial recognition technologies for racial and ethnic profiling. […]

Report of the Special Rapporteur on contemporary forms of slavery, including its causes and consequences, UN Doc A/78/161 (12 July 2023)

30. However, close consideration should be given to the potential unintended consequences of legislative and policy responses to contemporary forms of slavery. For instance, technology-mediated surveillance has been applied by law enforcement and other entities to "protect" potential victims and "rescue" those identified as victims of contemporary forms of slavery. However, surveillance in the context of anti-slavery efforts has been used in some countries to disproportionately scrutinize specific individuals, including those who intend to migrate abroad. This

has affected in particular women, among them sex workers.

41. […] Intelligence gathering must also be free from gender, racial or other bias in order not to stigmatize particularly vulnerable victims of contemporary forms of slavery, such as women, children, minorities, Indigenous peoples, migrants and persons with disabilities.

Report of the Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health, 'Digital innovation, technologies and the right to health', UN Doc A/HRC/53/65 (21 April 2023)

62. Insufficient protection for digital health data can leave marginalized groups vulnerable to criminalization, stigma, discrimination and violence. In certain circumstances, and depending on the legal framework in place, companies and even public sector bodies can be compelled by law enforcement bodies or courts to hand over personal data for criminal investigation purposes, without sufficient safeguards. Poor, minority racial and ethnic communities are disproportionately targeted and subject to surveillance, which could be exacerbated where health status is criminalized. That leads to them being disproportionately represented in the criminal justice systems of States and such individuals often face harsher punishments as a result of racial profiling and overpolicing compared to more affluent communities.

85. Digital technologies can improve access for individuals who face discrimination and/or otherwise lack access to health facilities, goods and services. However, the use of digital technologies, without sufficient human rights safeguards, also deepens and exacerbates existing inequalities. Vulnerable groups who face multiple forms of discrimination and oppression in some cases lack access to digital technology and face criminalization, stigmatization and State surveillance.

99. States must embed human rights principles of equality, non-discrimination, participation, transparency and accountability in implementation, in order to meet their obligations to respect, protect and fulfil the right to health in relation to digital innovation and technologies.

100. An intersectional rights-based approach to digital innovation and technologies must be adopted to move towards substantive equality and create the conditions conducive to a life of dignity.

Report of the Working Group on Discrimination Against Women and Girls, Women's and Girls' Sexual and Reproductive Health Rights in Crisis, UN Doc A/HRC/47/38 (28 April 2021)

67. Racism within the health system can be intensified by widespread State policing and surveillance and mandatory reporting requirements in relation to suspicions of drug use and child abuse or neglect, which often deters pregnant women from seeking reproductive health care and undermines their trust in health service providers. […]"

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Disinformation and Freedom of Opinion and Expression, UN Doc A/HRC/47/25 (13 April 2021)

66. Algorithms, targeted advertising and the data harvesting practices of the largest social media companies are largely credited with driving users towards "extremist" content and conspiracy theories that undermine the right to form an opinion and freedom of expression. There is a real concern that the systematic collection of data about users' activities online and targeted advertising may violate their right to freedom of opinion under article 19 (1) of the International Covenant on Civil and Political Rights. The lack of transparency with which companies automatically curate content online also points towards an unacceptable level of intrusion into individuals' right to form their ideas free from manipulation and right to privacy. […] Finally, there is evidence to suggest that the recording of people's private thoughts as expressed through online searches and other online activities could be used against them by commercial actors or Governments in a discriminatory

manner."

Report of the Special Rapporteur on Freedom of Religion or Belief, Countering Islamophobia/Anti-Muslim Hatred to Eliminate Discrimination and Intolerance Based on Religion or Belief, UN Doc A/HRC/46/30 (13 April 2021)

24. States have reportedly incorporated their essential services, including education and health care, within their national security apparatus in a way that disproportionately heightens surveillance of Muslims and potentially compounds existing inequalities, including educational and health outcomes. […]

28. […] It was also reported to the Special Rapporteur that law enforcement and intelligence officers in some Western countries surveil mosques and their attendees in the name of counter-terrorism.

79. States should: […] (c) Implement the recommendation made by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism to ensure that all policies aimed at preventing and countering violent extremism are governed by a clear and human rights-compliant legal framework and subject to rigorous monitoring and evaluation, including regular, independent and periodic review; […] (e) Counter discrimination through law enforcement, including by eliminating the discriminatory profiling of Muslims and promoting fair policing; taking measures to enhance the ability of law enforcement to recognize anti-Muslim bias; and increasing the enforcement of hate crime laws; […] (h) Ensure the existence of accessible and confidential mechanisms where victims can report incidences of Islamophobic hate crime and discrimination. Where such mechanisms exist, States must ensure that they are easily accessible and function in accordance with a victim-based human rights approach, including within the criminal justice system;

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Human Rights Impact of Counter-Terrorism and Countering (Violent) Extremism Policies and Practices on the Rights of Women, Girls and the Family, UN Doc A/HRC/46/36 (22 January 2021)

11. […] When surveillance is unlawfully undertaken, the individual harms are clear and often the focus of rights discussions, yet, in counter-terrorism operations, the family and home space are often part and parcel of those surveillance measures. […] Significant research has uncovered wide misuse and abuse of surveillance laws on a discriminatory basis, targeting particular communities and groups based on ethnic background, race and religion. […] Bodies of research have not only uncovered direct rights violations, but also how surveillance "produces fear and furthers control and securitization", compounds harm and alters the social fabric of tolerance towards increased suspicion and more permissive environments for hate speech and crimes. […]

26. […] As noted in previous country reports, the mothers of individuals who have committed terrorist attacks are subjected to intersecting intrusions by the State, violating not only the right to non-discrimination and privacy but also fundamentally disrupting the right to family life for extended periods. […]

Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, UN Doc A/75/590 (10 November 2020)

12. Autonomous technologies are also increasingly used in monitoring and securing border spaces. […] Such pushbacks likely violate non-refoulement obligations under international law, and are aided by surveillance technologies. One submission highlighted legal developments in Greece that permit the police to use drone surveillance to monitor irregular migration in border regions, but that do so without ensuring the requisite legal protections for the human rights of those subject to this surveillance.

27. In Austria, Belgium, Denmark, Germany, Norway and the United Kingdom of Great Britain and Northern Ireland, laws allow for the seizure of mobile phones from asylum or migration applicants, from which data are then extracted and used as part of asylum procedures. These practices constitute a serious, disproportionate interference with migrants' and refugees' right to privacy, on the basis of immigration status and, in effect, national origin. Furthermore, the presumption that data obtained from digital devices necessarily leads to reliable evidence is flawed. […] Some of these activities are undertaken directly by government officials themselves, but in some instances, governments call on companies to provide them with the tools and/or know-how to undertake this surveillance.

32. […] Surveillance humanitarianism refers to "enormous data collection systems deployed by aid organizations that inadvertently increase the vulnerability of people in urgent need". […] Potential harms around data privacy are often latent and violent in conflict zones, where data compromised or leaked to a warring faction could result in retribution for those perceived to be on the wrong side of the conflict.

34. Collection of vast amounts of data on migrants and refugees creates serious issues and possible human rights violations related to data sharing and access, particularly in settings such as refugee camps […]. Data collection and the use of new technologies, particularly in contexts characterized by steep power differentials, raise issues of informed consent and the ability to opt out.

35. […] A serious concern in this context is that of "function creep", where data collected in one context (e.g. monitoring low- level fraud) is shared and reused for different purposes (e.g. to populate registries of potential terror suspects), with no procedural and substantive protections for the individuals whose data are being shared and repurposed.

36. In some cases, the very nature of data collection can produce profoundly discriminatory outcomes. […]

53. All this points to a trend in immigration surveillance where predictive models use artificial intelligence to forecast whether people with no ties to criminal activity will nonetheless commit crimes in the future. Yet, these predictive models are prone to creating and reproducing racially discriminatory feedback loops. Furthermore, racial bias is already present in the datasets on which these models rely. When discriminatory datasets are treated as neutral inputs, they lead to inaccurate models of criminality which then "perpetuate racial inequality and contribute to the targeting and overpolicing of non-citizens".

58. At both the domestic and international levels, Member States must ensure that border and immigration enforcement and administration are subject to binding legal obligations to prevent, combat and remedy racial and xenophobic discrimination in the design and use of digital border technologies. These obligations include but are not limited to: (b) An immediate moratorium on the procurement, sale, transfer and use of surveillance technology, until robust human rights safeguards are in place to regulate such practices. These safeguards include human rights due diligence that complies with international human rights law prohibitions on racial discrimination, independent oversight, strict privacy and data protection laws, and full transparency about the use of surveillance tools such as image recordings and facial recognition technology. In some cases, it will be necessary to impose outright bans on technology that cannot meet the standards enshrined in international human rights legal frameworks prohibiting racial discrimination;

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/43/52 (24 March 2020)

27. States and non-State actors should: (b) Respect, protect and facilitate the right to privacy to enable individuals to enjoy other rights, such as the rights to assemble and express opinions,

irrespective of their gender, by: (ii) Reducing infringements of privacy based on gender by: a. Adopting robust privacy and data protection laws and policies.

28. States should take all legislative, policy, administrative and other measures, in line with international human rights norms and standards, necessary to ensure that: (b) Privacy infringements based on gender, by public or private actors, are prevented by ensuring that: (iv) There is recognition of the responsibility to protect and warn in relation to patterns of extraterritorial outreach of States that violate the right to privacy; (v) Policies and procedures are up to date and adequately serve the obligation to protect and warn, and prevent surveillance and harassment based on gender, by foreign States and non-State actors against their citizens or non-citizens in their territories.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Human Rights Impact of Policies and Practices Aimed at Preventing and Countering Violent Extremism, UN Doc A/HRC/43/46 (21 February 2020)

32. Many practices for preventing and countering violent extremism involve targeting particular people, communities and groups, giving rise to assumptions about their "suspect", profiling, excluding and compounding structural discrimination and exclusion, including surveillance and harassment. […] Such policies lead to overselection and overreporting, largely on prohibited discriminatory grounds, having an impact on the rights to freedom of religion and expression and privacy. Furthermore, the lack of transparency about the use of the information generated and its often underregulated sharing across government entities lends credence to a perception that preventing and countering violent extremism is yet another tool of a State intelligence entity's counter-terrorism efforts, rather than a genuine effort at building resistance to the threat of violent extremism.

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/40/63 (27 October 2019)

78. Surveillance, unless undertaken lawfully, proportionately and necessarily represents infringements upon the human right to privacy. Gender, race, class, social origin, religion, opinions and their expression can become factors in determining who is watched in society, and make certain individuals more likely to suffer violations of their right to privacy.

Report of the Independent Expert on the Protection Against Violence and Discrimination Based on Sexual Orientation and Gender Identity, Data Collection and Management as a Means to Create Heightened Awareness of Violence and Discrimination Based on Sexual Orientation and Gender Identity, UN Doc A/HRC/41/45 (14 May 2019)

17. Human rights considerations demand careful management of the design and implementation of the processes for the collection and management of all personal information. In the areas of sexual orientation and gender identity the risks are exacerbated owing to the associated stigmatization in certain social contexts, which might create a motivation to hack or steal the data or otherwise unlawfully access it. Stigmatization also multiplies the damaging impact of disclosure of information due to negligence or mistakes. Information about sexual orientation and gender identity may be released through data sharing, particularly when administrative data is shared between agencies in the course of programme administration, or if the data collection methods themselves are not conducted in a safe space or are conducted in a manner indicating that the data collection effort targets lesbian, gay, bisexual, trans and gender-diverse persons.

22. By definition, full State diligence to prevent, prosecute and punish violence and discrimination based on sexual orientation and gender identity and expression is impossible in environments in which the State criminalizes certain forms of sexual orientation and gender identity and expression. In those environments, fully effective data collection, that is, data collection that serves the purpose

of addressing violence and discrimination, is also impossible. Indeed, in contexts such as those a presumption must exist that data is gathered for purposes that are contrary to international human rights law, a working theory supported by multiple accounts received by the mandate holder of data being used in such contexts as the basis for surveillance, harassment, entrapment, arrest and persecution by government officials.

26. The challenges to proper data collection must be identified and addressed. For example, there are no universally accepted standards determining the classification of sexual orientation and gender identity.

56. Conversely, the collection and management of data to enable criminal prosecution of same-sex relations or on the basis of sexual orientation and gender identity is, by definition, a violation of the principle of lawful use. The mandate holder has already concluded that legislation, public policy and jurisprudence that criminalize same-sex relationships and particular gender identities are per se contrary to international human rights law, and therefore any measures, including data collection and management, conducive to their implementation are equally contrary to international human rights law.

Report of the Special Rapporteur on Freedom of Religion or Belief, UN Doc A/HRC/40/58 (5 March 2019)

11. […] The Special Rapporteur wishes to raise concern about the many reports he has received detailing surveillance, intimidation, harassment, prosecution, threats of bodily harm, torture or murder following acts that had exceeded the limits imposed by law or social convention on peaceful manifestations of thoughts, conscience, and religion or belief, and/or that had offended the sensitivities of others by denigrating what they held sacred.

51. […] State attempts to combat incitement have contributed to the emergence of "digital authoritarianism" through increased surveillance, encroachment on privacy and broad restrictions on expression related to religion or belief, which has rendered cyberspace a perilous place for dissenters and religious minorities. Digital applications, for example, are reportedly being used to report allegations of blasphemy, and digital footprints can be used to assess compliance with faith-related observances. […]

52. […] While there is a need to prevent and punish online incitement to violence, some of the current approaches, characterized by vaguely worded laws on what is proscribed and draconian intermediary penalties, are likely to be highly counterproductive, with chilling effects. The negative impact of the rise of digital authoritarianism is evident from the high number of cases of murders, attacks and prosecutions that have resulted from online activity. At the same time, criminal and terrorist groups have recently demonstrated the potential for online platforms to be used to propagate violent religious extremism or to incite violence against religious minorities.

54. […] Individuals and whole communities may also be targeted through the manipulation of online filters, and the use of some tools, such as facial recognition technology, risks undermining the activities of civil society actors that peacefully pursue the exercise of fundamental human rights.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/HRC/34/61 (21 February 2017)

33. […] The Special Rapporteur recalls that differential treatment of nationals and non-nationals, and of those within or outside a State's jurisdiction, is incompatible with the principle of non-discrimination, which is a key constituent of any proportionality assessment.

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/71/368 (30 August 2016)

36. […] what is the true value of laws that discriminate between nationals and non-nationals? Especially since, in terms of article 17 of the International Covenant on Civil and Political Rights, everybody enjoys a right to privacy irrespective of nationality or citizenship, so one must ask how useful and appropriate, never mind legal, such types of provisions may be [...] This interpretation is as unacceptable as any claim in the laws of other countries that fundamental human rights protection is only restricted to its own citizens or residents.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014)

62. […] Moreover, article 26 of the Covenant prohibits discrimination on grounds of, inter alia, nationality and citizenship. The Special Rapporteur thus considers that States are legally obliged to afford the same privacy protection for nationals and non-nationals and for those within and outside their jurisdiction. Asymmetrical privacy protection regimes are a clear violation of the requirements of the Covenant.

Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee, UN Doc CCPR/C/POL/CO/7 (4 November 2016)

39. The Committee is concerned about the surveillance and interception powers of the Polish intelligence and law enforcement authorities as reflected in the Law on Counterterrorism of June 2016 and the Act amending the Police Act and certain other acts of January 2016. The Committee is particularly concerned about: [...] (b) the targeting of foreign nationals and application of different legal criteria to them.

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet OEA/Ser.L/V/II. CIDH/RELE/INF.11/13 (31 December 2013)

150. […] Moreover, the people most affected are those who take unpopular positions, or the members of political, racial, or religious minorities who are often unjustifiably classified as "terrorists", which makes them object of surveillance and monitoring without proper oversight. […]

163. When establishing [any limitations on the right to privacy], States must abstain from perpetuating prejudice and discrimination. Accordingly, limitations to the exercise of fundamental rights cannot be discriminatory or have discriminatory effects, as this would also be inconsistent with Articles 1.1 and 24 of the American Convention. It bears recalling that, under Article 13 of the American Convention, freedom of expression is a right that belongs to "everyone," and by virtue of Principle 2 of the Declaration of Principles, "[a]ll people should be afforded equal opportunities to receive, seek and impart information by any means of communication without any discrimination for reasons of race, color, sex, language, religion, political or other opinions, national or social origin, economic status, birth or any other social condition.

SECTION 5: MASS SURVEILLANCE PROGRAMMES

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

Noting that, while metadata may provide benefits, certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications and can give an insight into an individual's behaviour, social relationships, private preferences and identity, […]

Emphasizing that unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data, hacking and the unlawful use of biometric technologies, as highly intrusive acts, violate the right to privacy, […] including when undertaken extraterritorially or on a mass scale,"

Deeply concerned at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights,

7. *Calls upon* all States: (d) To review, on a regular basis, their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, as well as regarding the use of profiling, automated decision-making, machine learning and biometric technologies, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

** See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014)*

UN General Assembly Resolution on the Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc A/RES/72/180 (19 December 2017)

5. Urges States, while countering terrorism: (j) To review their procedures, practices and legislation regarding the surveillance and interception of communications and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law, and to take measures to ensure that interference with the right to privacy is regulated by law, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that such interference is not arbitrary or unlawful, bearing in mind what is reasonable for the pursuance of legitimate aims;

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

10. *Calls upon* all States: (c) To review, on a regular basis, their procedures, practices and legislation regarding the surveillance of communications, including mass surveillance and the interception and collection of personal data, as well as regarding the use of profiling, automated decision-making, machine learning and biometric technologies, with a view to upholding the right

to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

**See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019)*

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

17. Many States continue to engage in secret mass surveillance and communications interception, collecting, storing and analysing the data of all users relating to a broad range of means of communication (for example, emails, telephone and video calls, text messages and websites visited). While some States claim that such indiscriminate mass surveillance is necessary to protect national security, this practice is "not permissible under international human rights law, as an individualized necessity and proportionality analysis would not be possible in the context of such measures" (see A/HRC/33/2 9, para. 58).

18. States often rely on business enterprises for the collection and interception of personal data. For example, some States compel telecommunications and Internet service providers to give them direct access to the data streams running through their networks. Such systems of direct access are of serious concern, as they are particularly prone to abuse and tend to circumvent key procedural safeguards. Some States also demand access to the massive amounts of information collected and stored by telecommunications and Internet service providers. States continue to impose mandatory obligations on telecommunications companies and Internet service providers to retain communications data for extended periods of time. Many such laws require the companies to collect and store indiscriminately all traffic data of all subscribers and users relating to all means of electronic communication. They limit people's ability to communicate anonymously, create the risk of abuses and may facilitate disclosure to third parties, including criminals, political opponents, or business competitors through hacking or other data breaches. Such laws exceed the limits of what can be considered necessary and proportionate. […]

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

26. Concerns about whether access to and use of data are tailored to specific legitimate aims also raise questions about the increasing reliance of Governments on private sector actors to retain data "just in case" it is needed for government purposes. Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate. […]

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014)

In the context of targeted surveillance, whichever method of prior authorization is adopted (judicial or executive), there is at least an opportunity for ex ante review of the necessity and proportionality of a measure of intrusive surveillance by reference to the particular circumstances of the case and the individual or organization whose communications are to be intercepted. Neither of these opportunities exists in the context of mass surveillance schemes since they do not depend on individual suspicion. Ex ante review is thus limited to authorizing the continuation of the scheme as a whole, rather than its application to a particular individual [...]

18. Assuming therefore that there remains a legal right to respect for the privacy of digital communications (and this cannot be disputed (see General Assembly resolution 68/167)), the adoption of mass surveillance technology undoubtedly impinges on the very essence of that right. It is potentially inconsistent with the core principle that States should adopt the least intrusive means available when entrenching on protected human rights; it excludes any individualized proportionality assessment; and it is hedged around by secrecy claims that make any other form of proportionality analysis extremely difficult. The States engaging in mass surveillance have so far failed to provide a detailed and evidence-based public justification for its necessity, and almost no States have enacted explicit domestic legislation to authorize its use. Viewed from the perspective of article 17 of the Covenant, this comes close to derogating from the right to privacy altogether in relation to digital communications. For all these reasons, mass surveillance of digital content and communications data presents a serious challenge to an established norm of international law. In the view of the Special Rapporteur, the very existence of mass surveillance programmes constitutes a potentially disproportionate interference with the right to privacy. Shortly put, it is incompatible with existing concepts of privacy for States to collect all communications or metadata all the time indiscriminately. The very essence of the right to the privacy of communication is that infringements must be exceptional, and justified on a case-by-case basis.

36. Accessibility requires not only that domestic law be published, but also that it meet a standard of clarity and precision sufficient to enable those affected to regulate their conduct with foresight of the circumstances in which intrusive surveillance may occur... Prior to the introduction of mass surveillance programmes outlined in the present report, [it had always been understood that it was required for] domestic legislation to spell out clearly the conditions under which, and the procedures by which, any interference may be authorized; the categories of person whose communications may be intercepted; the limits on the duration of surveillance; and the procedures for the use and storage of the data collected. […]

52. The technical ability to run vast data collection and analysis programmes undoubtedly offers an additional means by which to pursue counter-terrorism and law enforcement investigations. But an assessment of the proportionality of these programmes must also take account of the collateral damage to collective privacy rights. Mass data collection programmes appear to offend against the requirement that intelligence agencies must select the measure that is least intrusive on human rights (unless relevant States are in a position to demonstrate that nothing less than blanket access to all Internet-based communication is sufficient to protect against the threat of terrorism and other serious crime). Since there is no opportunity for an individualized proportionality assessment to be undertaken prior to these measures being employed, such programmes also appear to undermine the very essence of the right to privacy. They exclude altogether the "case-by-case" analysis that the Human Rights Committee has regarded as essential, and they may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. The Special Rapporteur, accordingly, concludes that such programmes can be compatible with article 17 of the Covenant only if relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people in any part of the world. [...]

59. The prevention and suppression of terrorism is a public interest imperative of the highest importance and may in principle form the basis of an arguable justification for mass surveillance of the Internet. However, the technical reach of the programmes currently in operation is so wide that they could be compatible with article 17 of the Covenant only if relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people located in any part of the world. Bulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of

the right guaranteed by article 17. In the absence of a formal derogation from States' obligations under the Covenant, these programmes pose a direct and ongoing challenge to an established norm of international law.

60. […] there is an urgent need for States using [Mass Surveillance] technology to revise and update national legislation to ensure consistency with international human rights law. Not only is this a requirement of Article 17, but it also provides an important opportunity for informed debate that can raised public awareness and enable individuals to make informed choices. Where the privacy rights of the entire digital community are at stake, nothing short of detailed and explicit primary legislation should suffice.

63. The Special Rapporteur calls upon all States that currently operate mass digital surveillance technology to provide a detailed and evidence-based public justification for the systematic interference with the privacy rights of the online community by reference to the requirements of article 17 of the Covenant. States should be transparent about the nature and extent of their Internet penetration, its methodology and its justification, and should provide a detailed public account of the tangible benefits that accrue from its use.

Concluding Observations on the Fifth Periodic Report of the Netherlands, Human Rights Committee, UN Doc CCPR/C/NLD/CO/5 (22 August 2019)

54. The Committee is concerned about the Intelligence and Security Services Act 2017, which provides the intelligence and security services with sweeping surveillance and interception powers, including bulk data collection. It is particularly concerned that the Act does not provide for a clear definition of case-specific bulk data collection; clear grounds for extending retention periods for information collected; and adequate safeguards against bulk data hacking. It is also concerned by the limited practical possibilities for complaining, in the absence of a comprehensive notification regime, to the Review Committee on the Intelligence and Security Services (art. 17).

Concluding Observations on the Sixth Periodic Report of Hungary, Human Rights Committee, UN Doc CCPR/C/HUN/CO/6 (9 May 2018)

43. The Committee is concerned that the State party's legal framework on secret surveillance for national security purposes (section 7/E (3) surveillance): (a) allows for mass interception of communications; and (b) contains insufficient safeguards against arbitrary interference with the right to privacy. It is also concerned at the lack of provision for effective remedies in cases of abuse and the absence of a requirement to notify the person under surveillance as soon as possible, without endangering the purpose of the restriction, after the termination of the surveillance measure (arts. 2, 17, 19 and 26).

44. The State party should increase the transparency of the powers of the legal framework on secret surveillance for national security purposes (section 7/E (3) surveillance) and the safeguards against its abuse by considering the possibility of making its policy guidelines and decisions public, in full or in part, subject to national security considerations and the privacy interests of individuals concerned by those decisions. It should ensure that all laws and policies regulating secret surveillance are in full conformity with its obligations under the Covenant, in particular article 17, including the principles of legality, proportionality and necessity; that effective and independent oversight mechanisms for secret surveillance are put in place; and that the persons affected have proper access to effective remedies in cases of abuse.

Concluding Observations on the Third Periodic Report of Lebanon, Human Rights Committee, UN Doc CCPR/C/LBN/CO/3 (9 May 2018)

33. The Committee is concerned about reports of arbitrary interference with the privacy of individuals, including allegations of mass surveillance of digital communications; […]

34. The State party […] should, inter alia, ensure that (a) surveillance, collection of, access to and use of data and communications data are tailored to specific legitimate aims, are limited to a specific number of persons and are subject to judicial authorization; […]

***Škoberne v Slovenia*, App No 19920/20, Judgment, European Court of Human Rights (15 February 2024)**

119. The Court reiterates that in view of the technological and social developments in the sphere of electronic communications, communications data can nowadays reveal a great deal of personal information. If obtained by the authorities in bulk, such data can be used to paint an intimate picture of a person through, *inter alia*, the mapping of social networks, location tracking, mapping of communication patterns, and insight into who that person has interacted with (see *Centrum för rättvisa*, § 256, and *Big Brother Watch and Others*, § 342, both cited above). The acquisition of such data through bulk interception can therefore be just as intrusive as the bulk acquisition of the content of communications, which is why their interception, retention and search by the authorities must be analysed by means of reference to the same safeguards as those applicable to content (see *Centrum för rättvisa*, § 277, and *Big Brother Watch and Others*, § 363, both cited above). This finding applies also to the general retention of communications data by communications service providers and its access by the authorities in individual cases, which must be accompanied, *mutatis mutandis*, by the same safeguards as those pertaining to secret surveillance (see *Ekimdzhiev and Others*, cited above, § 395).

123. […] Within the same context the Court has found that to minimise the risk of the bulk interception being abused, the process must be subject to "end-to-end safeguards" – meaning that (i) at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken, (ii) bulk interception should be subject to independent authorisation at the outset, when the object and scope of the bulk operation are being defined, and (iii) the operation should be subject to supervision and independent *ex post facto*review (see *Big Brother Watch and Others*, § 350, and *Centrum för rättvisa*, § 264, both cited above).

125. […] The issue that raises concerns with respect to Article 8 in the present case is, however, the regime underpinning the collocation of telecommunications data from which those relating to the applicant were obtained for the purposes of the criminal proceedings against him. In order to ascertain whether the interference constituted by that retention was "in accordance with the law" and proportionate, the Court must assess the Slovenian law governing data retention that was in force at the time in question.

126. […] The aforementioned provision required electronic communications providers to retain for a period of fourteen months, *inter alia*, communications data relating to fixed and mobile telephony for a number of purposes – namely for the purposes of criminal procedure and of ensuring national security, constitutional order, and the security, political and economic interests of the State and of the national defence. It must be emphasised that the applicant's data was not retained for the specific purpose of preventing or investigating serious crime but for any of the aforementioned purposes. The interference with his Article 8 rights constituted by the retention of his data must therefore be assessed within this broader context.

132. The present case does not concern a direct interception of data by the authorities, although it does relate to the risks of such interception. Under the impugned legal provisions, service providers were legally required to collect and store telecommunications data (beyond the extent

necessary for billing or other contractual purposes) in order to have them available for the authorities. Most of these data were likely never consulted. […]

133. However, unlike the case of *Breyer*, which concerned an interference of a limited nature (ibid., § 95), the present case concerns telecommunications data (see section 107.b of the Amended 2004 Act, cited in paragraph 64 above) which, when linked to a subscriber or a user, can reveal intimate pictures of his or her life through the mapping of social networks, location tracking, the mapping of communication patterns, and insight into who they have interacted with (see *mutatis mutandis*, *Ekimdzhiev and Others*, § 394; *Centrum för rättvisa*, § 256; and *Big Brother Watch and Others*, § 342, all cited above). In the Court's view, the systemic surveillance entailed by the mandatory retention of telecommunications data presents an impediment to the enjoyment of the privacy rights of all users of telecommunication services. The existence of large collections of telecommunications data and the ongoing retention of such data could understandably generate a sense of vulnerability and exposure and could prejudice persons' ability to enjoy privacy and the confidentiality of correspondence, to develop relations with others and to exercise other fundamental rights. In this regard the Court also refers to the observations made by the CJEU in *Digital Rights Ireland and Others* – namely, that communications data, taken as a whole, might allow "very precise conclusions to be drawn concerning the private lives of the persons whose data had been retained", and that its retention and processing therefore constituted "a wide-ranging and particularly serious interference" with their fundamental rights (see paragraph 76 above). The severity of the interference was acknowledged also by the respondent Government (see paragraph 117 above) and the Slovenian Constitutional Court (see paragraphs 55 and 66-68 above).

137. The Court notes that while the legal provisions governing the treatment of communications data might be different from those governing the surveillance of the content of communication, they should be analysed with reference to the same safeguards as those applicable to the content itself (see, *mutatis mutandis, Big Brother Watch and Others*, cited above, § 416). Therefore, the general retention of communications data by communications service providers and its access by the authorities in individual cases must be accompanied, *mutatis mutandis*, by the same safeguards as secret surveillance (*Ekimdzhiev and Others*, cited above, § 395). In its case-law on surveillance measures within the context of criminal investigations, the Court has developed the following minimum safeguards, which should be set out in law in order to avoid abuses of power: the nature of offences that may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which intercepted data may or must be erased or destroyed (see *Weber and Saravia v. Germany*(dec.), no. 54934/00, ECHR 2006 XI, and Liberty and Others v. the United Kingdom, no. 58243/00, 1 July 2008). In *Roman Zakharov* (cited above, § 231) – which concerned, in addition, other public-interest aims, such as the protection of national security – the Court framed the applicable safeguards along similar lines, with further emphasis placed on the notification mechanisms and the remedies provided by national law. It based its assessment of the compliance of the interception measures in question with Article 8 on the following criteria: the accessibility of the relevant domestic law; the scope and duration of the secret surveillance measures; the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data; the authorisation procedures; the arrangements for supervising the implementation of secret surveillance measures; and any notification mechanisms and the remedies provided by national law (ibid., § 238). Within the context of bulk interception relating to international communications, in *Big Brother Watch and Others* (cited above, § 361) and *Centrum för rättvisa* (cited above, § 275), the Court further adjusted the aforementioned criteria – including the requirement that the domestic law clearly define the grounds on which bulk interception may be authorised, the circumstances in which an

individual's communications may be intercepted and the procedure to be followed for granting authorisation.

138. As regards the present case, the Court observes that the Amended 2004 Act required, for several public-interest purposes, the retention for a period of fourteen months of all communications data generated or processed during the provision of related public communications services (see paragraph 64 above). The law did not seem to leave any decision in this respect to the discretion of any State or non-State body and was not ambiguous as to its application. Every individual or entity using the services of the telecommunications providers in Slovenia could anticipate that their telecommunications data was being retained as part of extensive data collection. However, the unambiguity of the law, which set out as a rule the general and indiscriminate retention of telecommunications data, could not be taken as constituting a sufficient guarantee of its compliance with the principles of rule of law and proportionality.

139. […] in the present case the applicant specifically complained of the retention of telecommunications data and the subsequent use of data that had been allegedly retained in breach of Article 8 (see paragraphs 125 and 126 above). The Court notes in this connection that the Amended 2004 Act set out a number of purposes for which the telecommunications data was to be retained, but it contained no provisions circumscribing the scope and application of the measure in relation to that which was necessary to achieve those purposes. Neither has it been shown that any other legislative act contained such provisions. It follows from the above-cited case-law (see paragraphs 119-123 and 137 above) that the national law should, as part of the minimum requirements, in a manner suitable to the particular form of surveillance, define the scope of application of the measure in question and provide appropriate procedures for ordering and/or reviewing it with a view to keeping it within the bounds of what is necessary. Having regard to the nature of the interference at issue (see paragraphs 132-134 above), those minimum requirements should have been met also by a measure entailing the retention of telecommunications data. The absence of provisions or mechanisms aimed at ensuring that the measure was actually limited to what was "necessary in a democratic society" for the specific purposes listed in the Amended 2004 Act rendered such a regime irreconcilable with the State's obligations under Article 8. The mere limitation of the retention to fourteen months, which is a considerable period, cannot undermine this conclusion.

143. The Court further notes that despite the applicant having clearly argued that the telecommunications data relating to his telecommunications had been retained in breach of his privacy rights, the domestic courts limited their assessment almost exclusively to the grounds on which the judicial orders had authorised access to the retained data – even though those grounds (as noted by the Constitutional Court) had not been challenged by the applicant (see paragraph 55 above). The Court would emphasise in this connection that even though the access to his data was accompanied by certain safeguards (such as judicial oversight), these safeguards, while being among the criteria that must be met (see *Ekimdzhiev and Others*, cited above, §§ 360-421), were not in themselves sufficient to render the retention regime compliant with Article 8. It notes by way of comparison that the CJEU similarly held in *SpaceNet and Telekom Deutschland* that national legislation that ensured full respect for the conditions established by its case-law interpreting the Data Retention Directive regarding access to retained data could not, by its very nature, be capable of either limiting or even remedying a serious interference resulting from the general retention of such data, the retention of and access to such data being separate interferences requiring separate justifications (see paragraph 87 above).

144. The applicant also argued that on account of the unjustified retention of his data, their acquisition and use in the domestic proceedings had violated Article 8 (see paragraphs 115 and 116 above). In this connection, the Court considers that when the retention of telecommunications data is found to violate Article 8 because it does not respect the "quality of law" requirement and/or the principle of proportionality, access to such data – and its subsequent

processing and storage by the authorities – could not, for the same reason, comply with Article 8. In this connection, reference may again be made to the view expressed by the CJEU. In *An Garda Síochána and Others* the CJEU found that communications data could not be the object of general and indiscriminate retention for the purpose of combating serious crime and that therefore, access to such data could not be justified for that same purpose (see paragraph 84 above). The Court sees no reason to find otherwise in respect of the applicant's case.

***Ekimdzhiev and Ors v Bulgaria*, App No 70078/12, Judgment, European Court of Human Rights (11 January 2022)**

356. Although significantly improved after they were examined by the Court in *Association for European Integration and Human Rights and Ekimdzhiev* (cited above), the laws governing secret surveillance in Bulgaria, as applied in practice, still fall short of the minimum safeguards against arbitrariness and abuse required under Article 8 of the Convention in the following respects: (a) the internal rules governing the storage and destruction of materials obtained via surveillance have not been made accessible to the public (see paragraph 296 *in fine* above); (b) the term "objects" in section 12(1) of the 1997 Act is not defined in a way so as ensure that it cannot serve as a basis for indiscriminate surveillance (see paragraph 303 above); (c) the excessive duration of the initial authorisation for surveillance on national-security grounds – two years – significantly weakens the judicial control to which such surveillance is subjected (see paragraph 305 above); (d) the authorisation procedure, as it operates in practice, is not capable of ensuring that surveillance is resorted to only when "necessary in a democratic society" (see paragraphs 307 to 322 above); (e) a number of lacunae exist in the statutory provisions governing the storing, accessing, examining, using, communicating and destroying of surveillance data (see paragraphs 326 to 332 above); (f) the oversight system, as currently organised, does not comply with the requirements of sufficient independence, competence and powers (see paragraphs 335 to 347 above); (g) the notification arrangements are too narrow (see paragraphs 349 to 351 above); and (h) the dedicated remedy, a claim under section 2(1)(7) of the 1988 Act, is not available in practice in all possible scenarios, does not ensure examination of the justification of each instance of surveillance (by reference to reasonable suspicion and proportionality), is not open to legal persons, and is limited in terms of the relief available (see paragraphs 266 to 273 and 352 to 355 above).

357. Those shortcomings in the legal regime appear to have had an actual impact on the operation of the system of secret surveillance in Bulgaria. The recurring scandals relating to secret surveillance (see paragraphs 56, 57, 59 and 67 above) suggest the existence of abusive surveillance practices, which appear to be at least in part due to the inadequate legal safeguards (see *Association for European Integration and Human Rights and Ekimdzhiev*, § 92, and *Roman Zakharov*, 303, both cited above).

358. It follows that the Bulgarian laws governing secret surveillance do not fully meet the "quality of law" requirement and are incapable of keeping the "interference" entailed by the system of secret surveillance in Bulgaria to what is "necessary in a democratic society". […]

372. It is settled that the mere storing of data relating to someone's private life amounts to interference with that individual's right to respect for his or her "private life" (see, with respect to personal data relating to the use of communications services, *Breyer v. Germany*, no. 50001/12, § 81, 30 January 2020; *Centrum för rättvisa*, cited above, § 244, and *Big Brother Watch and Others*, cited above, § 330). All types of communications data at issue in the present case – subscriber, traffic and location data – can relate, alone or in combination, to the "private life" of those concerned. Bulgarian law requires all communications service providers in the country to retain the entirety of that data of all users for potential subsequent access by the authorities (see paragraph 161 above). It has not been disputed that the two individual applicants use such services. It follows that this legally mandated retention is in itself an interference with their right

to respect for their "private life", irrespective of whether the retained data are then accessed by the authorities.

373. That retention amounts also to interference with those applicants' right to respect for their correspondence. The Court has already held that the storage of traffic and location data relating to a mobile telephone line amounts to interference with the right of the person using that line to respect for his "correspondence" (see *Ben Faiza v. France*, no. 31446/12, § 66-67, 8 February 2018). There is no reason to hold otherwise with respect to other types of communications, such as electronic communications, or with respect to communications data more generally. […]

394. In view of the technological and social developments in the past two decades in the sphere of electronic communications, communications data can nowadays reveal a great deal of personal information. If obtained by the authorities in bulk, such data can be used to paint an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who that person has interacted with (see *Centrum för rättvisa*, 256, and *Big Brother Watch and Others*, § 342, both cited above). The acquisition of that data through bulk interception can therefore be just as intrusive as the bulk acquisition of the content of communications, which is why their interception, retention and search by the authorities must be analysed by reference to the same safeguards as those applicable to content (see *Centrum för rättvisa*, § 277, and *Big Brother Watch and Others*, § 363, both cited above). […]

398. In Bulgaria, the law sets outs in an exhaustive manner the grounds on which the authorities may seek access to retained communications data: protecting national security; preventing, detecting or investigating serious criminal offences; tracing people finally sentenced to imprisonment with respect to such offences; tracing people who have fallen or could fall into a situation which puts their life or health at risk; and (only as concerns location data) carrying out search-and-rescue operations with respect to people in distress (see paragraph 163 above). The law is thus sufficiently clear on that point. As noted in paragraph 301 above in relation to secret surveillance, the mere fact that one of the grounds for accessing retained communications data is "national security" is not in itself contrary to Article 8 of the Convention.

419. Although the laws governing the retention of communications data and its subsequent accessing by the authorities were significantly improved after the Constitutional Court examined them in 2015 in the wake of the CJEU's judgment in *Digital Rights Ireland and Others* (see paragraph 156 above), those laws, as applied in practice, still fall short of the minimum safeguards against arbitrariness and abuse required under Article 8 of the Convention in the following respects:
(a) the authorisation procedure does not appear capable of ensuring that retained communications data is accessed by the authorities solely when that is "necessary in a democratic society" (see paragraphs 400 to 406 above);
(b) no clear time-limits have been laid down for destroying data accessed by the authorities in the course of criminal proceedings (see paragraph 408 above);
(c) no publicly available rules exist on the storing, accessing, examining, using, communicating and destroying communications data accessed by the authorities (see paragraph 409 above);
(d) the oversight system, as currently organised, does not appear capable of effectively checking abuse (see paragraphs 410 to 415 above);
(e) the notification arrangements, as currently operating, are too narrow (see paragraphs 416 and 417 above); and
(f) it does not appear that there is an effective remedy (see paragraphs 379 to 381 and 418 above).

420. It follows that those laws do not fully meet the "quality of law" requirement and are incapable of keeping the "interference" entailed by the system of retention and accessing of communications data in Bulgaria to what is "necessary in a democratic society".

***Big Brother Watch and Others v The United Kingdom*, Apps Nos 58170/13, 62322/14 and 24960/15, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

325. The Court views bulk interception as a gradual process in which the degree of interference with individuals' Article 8 rights increases as the process progresses. Bulk interception regimes may not all follow exactly the same model, and the different stages of the process will not necessarily be discrete or followed in strict chronological order. Nevertheless, subject to the aforementioned caveats, the Court considers that the stages of the bulk interception process which fall to be considered can be described as follows:

(a) the interception and initial retention of communications and related communications data (that is, the traffic data belonging to the intercepted communications);
(b) the application of specific selectors to the retained communications/related communications data;
(c) the examination of selected communications/related communications data by analysts; and
(d) the subsequent retention of data and use of the "final product", including the sharing of data with third parties.

330. The Court considers that Article 8 applies at each of the above stages. While the initial interception followed by the immediate discarding of parts of the communications does not constitute a particularly significant interference, the degree of interference with individuals' Article 8 rights will increase as the bulk interception process progresses. In this regard, the Court has clearly stated that even the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 […]. The fact that the stored material is in coded form, intelligible only with the use of computer technology and capable of being interpreted only by a limited number of persons, can have no bearing on that finding […].

347. […] While Article 8 of the Convention does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats, and States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary, for these purposes, in operating such a system the margin of appreciation afforded to them must be narrower and a number of safeguards will have to be present. […]

348. It is clear that the first two of the six "minimum safeguards" which the Court, in the context of targeted interception, has found should be defined clearly in domestic law in order to avoid abuses of power (that is, the nature of offences which may give rise to an interception order and the categories of people liable to have their communications intercepted), are not readily applicable to a bulk interception regime. Similarly, the requirement of "reasonable suspicion" […] is less germane in the bulk interception context, the purpose of which is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence. Nevertheless, the Court considers it imperative that when a State is operating such a regime, domestic law should contain detailed rules on when the authorities may resort to such measures. In particular, domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorised and the circumstances in which an individual's communications might be intercepted. The remaining four minimum safeguards defined by the Court in its previous judgments — that is, that domestic law should set out a limit on the duration of interception, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted data may or must be erased or destroyed — are equally relevant to bulk

interception.

349. […] In the context of bulk interception the importance of supervision and review will be amplified, because of the inherent risk of abuse and because the legitimate need for secrecy will inevitably mean that, for reasons of national security, States will often not be at liberty to disclose information concerning the operation of the impugned regime.

350. […] the Court considers that the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review. […]

351. […] Nevertheless, bulk interception should be authorised by an independent body; that is, a body which is independent of the executive. […]

352. […] the independent authorising body should be informed of both the purpose of the interception and the bearers or communication routes likely to be intercepted. This would enable the independent authorising body to assess the necessity and proportionality of the bulk interception operation and also to assess whether the selection of bearers is necessary and proportionate to the purposes for which the interception is being conducted.

354. Taking into account the characteristics of bulk interception (see paragraphs 344-345 above), the large number of selectors employed and the inherent need for flexibility in the choice of selectors, which in practice may be expressed as technical combinations of numbers or letters, the Court would accept that the inclusion of all selectors in the authorisation may not be feasible in practice. Nevertheless, given that the choice of selectors and query terms determines which communications will be eligible for examination by an analyst, the authorisation should at the very least identify the types or categories of selectors to be used.

355. […] The use of every such selector must be justified – with regard to the principles of necessity and proportionality – by the intelligence services and that justification should be scrupulously recorded and be subject to a process of prior internal authorisation providing for separate and objective verification of whether the justification conforms to the aforementioned principles.

356. […] the supervising body should be in a position to assess the necessity and proportionality of the action being taken, having due regard to the corresponding level of intrusion into the Convention rights of the persons likely to be affected. […]

358. The Court considers that a remedy which does not depend on notification to the interception subject could also be an effective remedy in the context of bulk interception; in fact, depending on the circumstances it may even offer better guarantees of a proper procedure than a system based on notification. Regardless of whether material was acquired through targeted or bulk interception, the existence of a national security exception could deprive a notification requirement of any real practical effect. The likelihood of a notification requirement having little or no practical effect will be more acute in the bulk interception context, since such surveillance may be used for the purposes of foreign intelligence gathering and will, for the most part, target the communications of persons outside the State's territorial jurisdiction. Therefore, even if the identity of a target is known, the authorities may not be aware of his or her location.

359. The powers and procedural guarantees an authority possesses are relevant in determining whether a remedy is effective. Therefore, in the absence of a notification requirement it is

imperative that the remedy should be before a body which, while not necessarily judicial, is independent of the executive and ensures the fairness of the proceedings, offering, in so far as possible, an adversarial process. […]"

360. In the light of the above, the Court will determine whether a bulk interception regime is Convention compliant by conducting a global assessment of the operation of the regime. Such assessment will focus primarily on whether the domestic legal framework contains sufficient guarantees against abuse, and whether the process is subject to "end-to-end safeguards" (see paragraph 350 above). In doing so, it will have regard to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse (see *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 92).

361. In assessing whether the respondent State acted within its margin of appreciation (see paragraph 347 above), the Court would need to take account of a wider range of criteria than the six *Weber* safeguards. More specifically, in addressing jointly "in accordance with the law" and "necessity" as is the established approach in this area (see *Roman Zakharov*, cited above, § 236 and *Kennedy*, cited above, § 155), the Court will examine whether the domestic legal framework clearly defined:

1. the grounds on which bulk interception may be authorised;
2. the circumstances in which an individual's communications may be intercepted;
3. the procedure to be followed for granting authorisation;
4. the procedures to be followed for selecting, examining and using intercept material;
5. the precautions to be taken when communicating the material to other parties;
6. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
8. the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.

362. Despite being one of the six *Weber* criteria, to date the Court has not yet provided specific guidance regarding the precautions to be taken when communicating intercept material to other parties. However, it is now clear that some States are regularly sharing material with their intelligence partners and even, in some instances, allowing those intelligence partners direct access to their own systems. Consequently, the Court considers that the transmission by a Contracting State to foreign States or international organisations of material obtained by bulk interception should be limited to such material as has been collected and stored in a Convention compliant manner and should be subject to certain additional specific safeguards pertaining to the transfer itself. First of all, the circumstances in which such a transfer may take place must be set out clearly in domestic law. Secondly, the transferring State must ensure that the receiving State, in handling the data, has in place safeguards capable of preventing abuse and disproportionate interference. In particular, the receiving State must guarantee the secure storage of the material and restrict its onward disclosure. This does not necessarily mean that the receiving State must have comparable protection to that of the transferring State; nor does it necessarily require that an assurance is given prior to every transfer. Thirdly, heightened safeguards will be necessary when it is clear that material requiring special confidentiality – such as confidential journalistic material – is being transferred. Finally, the Court considers that the transfer of material to foreign intelligence partners should also be subject to independent control."

370. In principle, the wider the grounds are, the greater the potential for abuse. However, narrower and/or more tightly defined grounds would only provide an effective guarantee against abuse if there were sufficient other safeguards in place to ensure that bulk interception was only authorised for a permitted ground and that it was necessary and proportionate for that purpose.

The closely related issue of whether there existed sufficient guarantees to ensure that the interception was necessary or justified is therefore as important as the degree of precision with which the grounds on which authorisation may be given are defined. Consequently, in the Court's view, a regime which permits bulk interception to be ordered on relatively wide grounds may still comply with Article 8 of the Convention, provided that, when viewed as a whole, sufficient guarantees against abuse are built into the system to compensate for this weakness.

***Centrum för Rättvisa v Sweden*, App No 35252/08, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)**

236. […] Unlike the targeted interception which has been the subject of much of the Court's case-law, and which is primarily used for the investigation of crime, bulk interception is also – perhaps even predominantly – used for foreign intelligence gathering and the identification of new threats from both known and unknown actors. When operating in this realm, Contracting States have a legitimate need for secrecy which means that little if any information about the operation of the scheme will be in the public domain, and such information as is available may be couched in terminology which is obscure and which may vary significantly from one State to the next.

237. […] the Court is required to carry out its assessment of Contracting States' bulk interception regimes, a valuable technological capacity to identify new threats in the digital domain, for Convention compliance by reference to the existence of safeguards against arbitrariness and abuse, on the basis of limited information about the manner in which those regimes operate.

253. […] the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law […].

258. To begin with, bulk interception is generally directed at international communications (that is, communications physically travelling across State borders), and while the interception and even examination of communications of persons within the surveilling State might not be excluded, in many cases the stated purpose of bulk interception is to monitor the communications of persons outside the State's territorial jurisdiction, which could not be monitored by other forms of surveillance.

262. […] Nevertheless, the Court considers it imperative that when a State is operating such a regime, domestic law should contain detailed rules on when the authorities may resort to such measures. In particular, domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorised and the circumstances in which an individual's communications might be intercepted. […]

268. Taking into account the characteristics of bulk interception (see paragraphs 258 and 259 above), the large number of selectors employed and the inherent need for flexibility in the choice of selectors, which in practice may be expressed as technical combinations of numbers or letters, the Court would accept that the inclusion of all selectors in the authorisation may not be feasible in practice. Nevertheless, given that the choice of selectors and query terms determines which communications will be eligible for examination by an analyst, the authorisation should at the very least identify the types or categories of selectors to be used."

275. In assessing whether the respondent State acted within its margin of appreciation (see paragraph 256 above), the Court would need to take account of a wider range of criteria than the six Weber safeguards. More specifically, in addressing jointly "in accordance with the law" and "necessity" as is the established approach in this area (see Roman Zakharov, cited above, § 236;

and Kennedy, cited above, § 155), the Court will examine whether the domestic legal framework clearly defined:

1. The grounds on which bulk interception may be authorised;
2. The circumstances in which an individual's communications may be intercepted;
3. The procedure to be followed for granting authorisation;
4. The procedures to be followed for selecting, examining and using intercept material;
5. The precautions to be taken when communicating the material to other parties;
6. The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
7. The procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
8. The procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.

276. Despite being one of the six *Weber* criteria, to date the Court has not yet provided specific guidance regarding the precautions to be taken when communicating intercept material to other parties. However, it is now clear that some States are regularly sharing material with their intelligence partners and even, in some instances, allowing those intelligence partners direct access to their own systems. Consequently, the Court considers that the transmission by a Contracting State to foreign States or international organisations of material obtained by bulk interception should be limited to such material as has been collected and stored in a Convention compliant manner and should be subject to certain additional specific safeguards pertaining to the transfer itself. First of all, the circumstances in which such a transfer may take place must be set out clearly in domestic law. Secondly, the transferring State must ensure that the receiving State, in handling the data, has in place safeguards capable of preventing abuse and disproportionate interference. In particular, the receiving State must guarantee the secure storage of the material and restrict its onward disclosure. This does not necessarily mean that the receiving State must have comparable protection to that of the transferring State; nor does it necessarily require that an assurance is given prior to every transfer. Thirdly, heightened safeguards will be necessary when it is clear that material requiring special confidentiality – such as confidential journalistic material – is being transferred. Finally, the Court considers that the transfer of material to foreign intelligence partners should also be subject to independent control."

311. The Court considers that the obligation to keep logs and detailed record of each step in bulk interception operations, including all selectors used, must be set out in domestic law. The fact that in Sweden it appears in internal instructions only is undoubtedly a shortcoming. However, having regard, in particular, to the existence of oversight mechanisms covering all aspects of the FRA's activities, there is no reason to consider that detailed logs and records are not kept in practice or that the FRA could proceed to changing its internal instructions arbitrarily and removing its obligation in that regard.

326. In the Court's view, despite the above considerations, the absence, in the relevant signals intelligence legislation, of an express legal requirement for the FRA to assess the necessity and proportionality of intelligence sharing for its possible impact on Article 8 rights is a substantial shortcoming of the Swedish regime of bulk interception activities. It appears that, as a result of this state of the law, the FRA is not obliged to take any action even in situations when, for example, information seriously compromising privacy rights is present in material to be transmitted abroad without its transmission being of any significant intelligence value. Furthermore, despite the fact that the Swedish authorities obviously lose control over the shared material once it has been sent out, no legally binding obligation is imposed on the FRA to analyse and determine whether the foreign recipient of intelligence offers an acceptable minimum level of safeguards (see paragraph 276 above).

330. […] the absence of a requirement in the Signals Intelligence Act or other relevant legislation

that consideration be given to the privacy interests of the individual concerned when making a decision about intelligence sharing is a significant shortcoming of the Swedish regime, to be taken into account in the Court's assessment of its compatibility with Article 8 of the Convention.

331. The duration of bulk interception operations is, of course, a matter for the domestic authorities to decide. There must, however, be adequate safeguards, such as a clear indication in domestic law of the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled (see *Roman Zakharov*, cited above, § 250).

335. The Court is of the view that an express provision on discontinuation of bulk interception when no longer needed would have been clearer than the existing arrangement in Sweden according to which, apparently, permits may or may not be cancelled when circumstances warranting such a cancellation come to light in the period before the expiry of their six months' validity.

336. The significance of this shortcoming should, however, not be overestimated, in the Court's view, for two main reasons. First, Swedish law provides for relevant mechanisms, such as the possibility for the requesting authority to revoke a tasking directive and for supervision by the Inspectorate, both of which can lead to the cancellation of a bulk interception mission when the conditions for it have ceased to exist or it is no longer needed. Second, by the nature of things, in the context of signals intelligence within foreign intelligence the implementation of a legal requirement to cancel a permit when no longer needed must in all likelihood be heavily dependent on internal operative assessments involving secrecy. Therefore, in the specific context of bulk interception for foreign intelligence purposes, the existence of supervision mechanisms with access to all internal information must generally be seen as providing similar legislative safeguards against abuse related to the duration of interception operations.

342. In the Court's view, while there is clear justification for special requirements regarding the destruction of material containing personal data, there must also be a general legal rule governing the destruction of other material obtained through bulk interception of communications, where keeping it may affect, for example, the right of respect for correspondence under Article 8, including concerning legal persons as the applicant. As a very minimum, as also stressed by the Chamber, there should be a legal requirement to delete intercepted data that has lost pertinence for signals intelligence purposes. The Government have not shown that the Swedish regulatory framework covers this aspect. However, while observing that there is only a narrow set of circumstances in which it could happen that none of the specific rules on destruction of intercept material noted in the preceding paragraphs would apply, the Court notes this point as a procedural shortcoming in the regulatory framework.

343. Finally, the Court does not have sufficient information as to the manner in which the necessity to keep or destroy material containing personal data is assessed in practice and as to whether unprocessed intercept material is always stored for the maximum period of one year or the necessity of continued storage is regularly reviewed, as it should be. This makes it difficult to arrive at comprehensive conclusions covering all aspects of the storage and deletion of intercept material. In the context of its analysis on the *ex post facto* review in the Swedish bulk interception system, the Court will return to the question what conclusions could be drawn from the fact that it has insufficient information on the above point and other aspects of the functioning of the Swedish system.

***Szabó and Vissy v Hungary*, App No 37138/14, Judgment, European Court of Human Rights (12 January 2016)**

In the face of this progress the Court must scrutinise the question as to whether the development

of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights. These data often compile further information about the conditions in which the primary elements intercepted by the authorities were created, such as the time and place of, as well as the equipment used for, the creation of computer files, digital photographs, electronic and text messages and the like. Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European Union and, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities' enhanced technical possibilities to intercept private information.

Commissioner Lawrence M. Mute, Vice-Chairperson of the African Commission on Human and Peoples' Rights and Special Rapporteur on Freedom of Expression and Access to Information in Africa, 65th Ordinary Session of the African Commission on Human and Peoples' Rights (21 October - 10 November 2019)

40. I also welcome the decision of the High Court of South Africa on 16 September 2019 declaring various sections of the Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002 (RICA) unconstitutional for failing to provide a procedure for notifying the subject of the interception; failure to address expressly the circumstances where a subject of surveillance is either a practising lawyer or a journalist; failure to prescribe proper procedures to be followed when State officials are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from interceptions; and failure to adequately provide for a system with appropriate safeguards to deal with the fact that the orders in question are granted ex parte. Bulk surveillance activities and foreign signals interception was also declared unlawful and invalid.

UN General Assembly Resolution on the Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc A/RES/72/180 (19 December 2017)

5. Urges States, while countering terrorism: (j) To review their procedures, practices and legislation regarding the surveillance and interception of communications and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law, and to take measures to ensure that interference with the right to privacy is regulated by law, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that such interference is not arbitrary or unlawful, bearing in mind what is reasonable for the pursuance of legitimate aims

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

Noting that the rapid pace of technological development enables individuals all over the world to use information and communications technology, and at the same time enhances the capacity of Governments, business enterprises and individuals to undertake surveillance, interception, hacking and data collection, which may violate or abuse human rights, in particular the right to privacy, and is therefore an issue of increasing concern,

8. *Calls upon* States: (c) To review, on a regular basis, their procedures, practices and legislation regarding the surveillance of communications, including mass surveillance and the interception and

collection of personal data, as well as regarding the use of profiling, automated decision-making, machine learning and biometric technologies, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

** See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/34/7 (23 March 2017)*

UN Human Rights Council Resolution on Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/HRC/RES/35/34 (23 June 2017)

20. *Urges* all States to respect and protect the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, including in the context of digital communication, and calls upon States, while countering terrorism and violent extremism conducive to terrorism, to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law, and *urges* them to take measures to ensure that any interference with the right to privacy is regulated by law, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that such interference is not arbitrary or unlawful, bearing in mind what is reasonable to the pursuance of legitimate aims;"

Report of the Human Rights Council Advisory Committee, Possible impacts, Opportunities and Challenges of New and Emerging Digital Technologies With Regard to the Promotion and Protection of Human Rights, UN Doc A/HRC/47/52 (19 May 2021)

25. Illegal and arbitrary forms of mass surveillance involving the indiscriminate monitoring of the entire or a significant portion of the population may emerge. All too often, surveillance is conducted without appropriate safeguards, which impinges unreasonably on the privacy and reputation of innocent people and harms the democratic norms of society.

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

44. One particular concern in public surveillance relates to the recording of photographic images. […] Recording, analysing and retaining facial images of individuals without their consent constitute interference with their right to privacy. By deploying facial recognition technology in public spaces, which requires the collection and processing of facial images of all persons captured on camera, such interference is occurring on a mass and indiscriminate scale.

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

18. States often rely on business enterprises for the collection and interception of personal data. For example, some States compel telecommunications and Internet service providers to give them direct access to the data streams running through their networks. Such systems of direct access are of serious concern, as they are particularly prone to abuse and tend to circumvent key procedural safeguards. Some States also demand access to the massive amounts of information collected and stored by telecommunications and Internet service providers. States continue to impose mandatory obligations on telecommunications companies and Internet service providers to retain communications data for extended periods of time. Many such laws require the companies to collect and store indiscriminately all traffic data of all subscribers and users relating to all means of electronic

communication. They limit people's ability to communicate anonymously, create the risk of abuses and may facilitate disclosure to third parties, including criminals, political opponents, or business competitors through hacking or other data breaches. Such laws exceed the limits of what can be considered necessary and proportionate. […]"

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

25. […] Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed. Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate.

26. Concerns about whether access to and use of data are tailored to specific legitimate aims also raise questions about the increasing reliance of Governments on private sector actors to retain data "just in case" it is needed for government purposes. Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate. […]

Report of the Working Group on Enforced and Involuntary Disappearances, 'New technologies and enforced disappearances', UN Doc A/HRC/54/22/Add.5 (11 September 2023)

22. The Working Group also observed with concern the uncontrolled proliferation of mass surveillance, facial-recognition and similar programmes. By nature, these systems subject a significant number of individuals to indiscriminate monitoring, systematically interfering with their human rights. The processing of biometric data, images and information gathered through these means by video-cameras in public spaces has been used to single out certain individuals, including in the context of social protests, who have subsequently been arrested and, in certain cases, forcibly disappeared. Centralised data systems operated through mobile applications used by governmental officials have been allegedly used to perform similar operations of mass surveillance, leading to the targeting of certain individuals considered to be 'suspicious' (including human rights defenders and persons belonging to ethnic or religious minorities) and to their subsequent enforced disappearance.

57. The Working Group is especially concerned at the use of Internet shutdowns and targeted connectivity disruptions; spyware programmes; targeted and mass surveillance, including gait and facial-recognition; cyberattacks and Government-sponsored troll factories; and the specious use of technology-related legislation to suppress dissent and target human rights defenders and relatives of disappeared persons.

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Human Rights Impact of Counter-Terrorism and Countering (Violent) Extremism Policies and Practices on the Rights of Women, Girls and the Family, UN Doc A/HRC/46/36 (22 January 2021)

11. The Special Rapporteur recalls the mandate's examination of how surveillance, particularly mass surveillance, for counter-terrorism purposes and access to bulk technology affects the right to privacy. She underscores that the right to privacy is a gateway right, enabling and supporting a range of other rights, including the exercise of the right to family life. She affirms that new technologies and data collection methods in particular have disparate impacts on minorities and are profoundly

gendered. New technologies that ease the operational burdens of surveillance and the investment in surveillance infrastructure that has developed since 11 September 2001 continue to grow at an exponential pace. […]

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/43/52 (24 March 2020)

52. States and non-State actors should: (a) Protect the privacy of digital communications and enjoyment of the right to privacy by all individuals, regardless of their gender, by promoting tools such as encryption; (b) Ensure that restrictions to the right to privacy, including through mass or targeted surveillance, requests for personal data or limitations on the use of encryption, pseudonymity and anonymity tools: (i) Are on a case-specific basis; (ii) Do not discriminate on the basis of gender or other factors, such as indigeneity; (iii) Are reasonable, necessary and proportionate as required by law for a legitimate purpose and ordered only by a court."

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, UN Doc A/HRC/41/41 (17 May 2019)

56. The proportionality principle requires proof that the measure used is the least invasive option. Mass surveillance or bulk collection and analysis of all communications metadata – explicitly designed to target associations between individuals – is inherently disproportionate. Similarly, legal requirements on communications service providers to store personal and sensitive data locally and register SIM cards on an indiscriminate basis allow authorities to access information which is not relevant and material to any serious crime or specific threat. […] Similarly, International Mobile Subscriber Identity capture devices (IMSI catchers) allow countries to collect data from thousands of mobile phones in a specific area, or at public events such as political demonstrations. Such practices are used to identify and surveil all individuals who participate in a particular event or are present in a certain public space. These forms of identification and data collection violate the individual's anonymity in public spaces and exert significant "chilling effects" on decisions to participate in public gatherings.

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/31/64 (8 March 2016)

39. The [Special Rapporteur on the Right to Privacy] firmly encourages the three committees of the UK Parliament commended above to continue, with renewed vigour and determination, to exert their influence in order that disproportionate, privacy-intrusive measures such as bulk surveillance and bulk hacking as contemplated in the Investigatory Powers Bill be outlawed rather than legitimised. It would appear that the serious and possibly unintended consequences of legitimising bulk interception and bulk hacking are not being fully appreciated by the UK Government... SRP invites the UK Government to show greater commitment to protecting the fundamental right to privacy of its own citizens and those of others and also to desist from setting a bad example to other states by continuing to propose measures, especially bulk interception and bulk hacking, which prima facie fail the standards of several UK Parliamentary Committees, run counter to the most recent Judgments of the European Court of Justice and the European Court of Human Rights, and undermine the spirit of the very right to privacy. […]

51. While some governments continue with ill-conceived, ill-advised, ill-judged, ill-timed and occasionally ill-mannered attempts to legitimise or otherwise hang on to disproportionate, unjustifiable privacy-intrusive measures such as bulk collection, bulk hacking, warrantless interception etc. other governments led, in this case by the Netherlands and the USA have moved more openly towards a policy of no back doors to encryption. The SRP would encourage many more governments to coalesce around this position.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/71/373 (6 September 2016)

20. […] Surveillance, including both bulk collection of data and targeted attacks on specific individuals or communities, interferes directly with the privacy and security necessary for freedom of opinion and expression, and always requires evaluation under article 19. […]

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/23/40 (17 April 2013)

62. […] Offensive intrusion software such as Trojans, or mass interception capabilities, constitute such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information. There are not just new methods for conducting surveillance; they are new forms of surveillance. From a human rights perspective, the use of such technologies is extremely disturbing. Trojans, for example, not only enable a State to access devices, but also enable them to alter – inadvertently or purposefully – the information contained therein. This threatens not only the right to privacy but also procedural fairness rights with respect to the use of such evidence in legal proceedings.

Concluding Observations on the Eighth Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/8 (26 March 2024)

53. […] [T]he State party should end the use of facial recognition and other mass surveillance technologies by law enforcement agencies at protests, in order to safeguard privacy, non-discrimination, freedom of expression and association and assembly rights for protesters.

Concluding Observations on the Eighth Periodic Report of Ukraine, UN Doc CCPR/C/UKR/CO/8 (11 November 2021)

42. The State party should bring its regulations governing data retention and access thereto, surveillance and interception activities into full conformity with the Covenant, in particular article 17, including with the principles of legality, proportionality and necessity. It should ensure that (a) any such interference with privacy requires prior authorization from a court and is subject to effective and independent oversight mechanisms; and (b) persons affected are notified of surveillance and interception activities, where possible, and have access to effective remedies in cases of abuse. The State party should also ensure that all reports of abuse are thoroughly investigated and that such investigations, where warranted, lead to appropriate sanctions.

Concluding Observations on the Seventh Periodic Report of Norway, Human Rights Committee, UN Doc CCPR/C/NOR/CO/7 (25 April 2018)

20. The Committee is concerned that amendments to the Code of Criminal Procedure and Police Act in 2016 grant broader monitoring and search powers to police, which may be used in a preventative manner to anticipate crime and may lack sufficient safeguards to prevent interference with the right to privacy. It is also concerned at reports about the intrusive use of satellite communications and of an ongoing proposal for a system of bulk data retention and its implications for the right to privacy (art. 17).

Concluding Observations on the Sixth Periodic Report of Denmark, Human Rights Committee, UN Doc CCPR/C/DNK/CO/6 (15 August 2016)

27. The Committee is concerned that the application of some of the measures used to combat terrorism may infringe the rights set forth in the Covenant. In particular, the Committee is concerned about: (b) section 780 of the Administration of Justice Act, which allows interception of communication by the police domestically and which may result in mass surveillance, despite the legal guarantees provided in sections 781 and 783 of the same Act […]

28. The State party should clearly define the acts that constitute terrorism in order to avoid abuses. The State party should ensure that the application of such legislation is compliant with the Covenant and that the principles of necessity, proportionality and non-discrimination are strictly observed.

Concluding Observations on the Initial Report of South Africa, Human Rights Committee, UN Doc CCPR/C/ZAF/CO/1 (27 April 2016)

42. […] The Committee is further concerned at reports of unlawful surveillance practices, including mass interception of communications carried out by the National Communications Centre […].

43. […] The State party should refrain from engaging in mass surveillance of private communications without prior judicial authorization. […]

Concluding Observations on the Sixth Periodic Report of Canada, Human Rights Committee, UN Doc CCPR/C/CAN/CO/6 (13 August 2015)

10. [T]he Committee is concerned about information according to which (a) Bill C-51 amendments to the Canadian Security Intelligence Act confers a broad mandate and powers on the Canadian Security Intelligence Service (CSIS) to act domestically and abroad, thus potentially resulting in mass surveillance and targeting activities that are protected under the Covenant without sufficient and clear legal safeguards. […] The State party should refrain from adopting legislation that imposes undue restrictions on the exercise of the rights under the Covenant. In particular, it should: Ensure its anti-terrorism legislation provides for adequate legal safeguards.

Commissioner for Human Rights, Council of Europe, Issue Paper on Democratic and Effective Oversight of National and Security Services, Commissioner's Recommendations (May 2015)

7. Require that security services obtain authorisation from a body that is independent from the security services and the executive, both in law and in practice, before engaging in any of the following activities either directly or through/in collaboration with private sector entities: (a) conducting untargeted bulk surveillance measures regardless of the methods or technology used or the type of communications targeted; (b) using selectors or key words to extract data from information collected through bulk surveillance, particularly when these selectors relate to identifiable persons; (c) collecting communications/metadata directly or accessing it through requests made to third parties, including private companies; (d) accessing personal data held by other state bodies; (e) undertaking computer network exploitation.

Concluding Observations on the Initial Report of Pakistan, Human Rights Committee, UN Doc CCPR/C/PAK/CO/1 (27 July 2017)

35. While noting the State party's view that the Prevention of Electronic Crimes Act 2016 complies with the Convention on Cybercrime, the Committee is concerned that the Act provides for […] (b) mandatory mass retention of traffic data by service providers for a minimum of one year […].

36. The State party should review its legislation on data collection and surveillance, in particular, the Prevention of Electronic Crimes Act 2016, to bring it in line with its obligations under the Covenant. It should… review all licensing requirements which impose obligations on network service providers to engage in communication surveillance, particularly in relation to indiscriminate data retention; and ensure that surveillance activities comply with its obligations under the Covenant. It should further adopt a comprehensive data protection law in line with international standards.

Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, UN Doc CCPR/C/ITA/CO/6 (28 March 2017)

36. […] [The Committee is concerned] that the Anti-Terrorism Decree and Law no 21/2016 ("Decreto Mille Proroghe") compel telecommunication providers to retain data beyond the period allowed by Article 132 of the Personal Data Protection Code, and accessing such data by the authorities is not subject to authorization from a judicial authority [...]

Concluding Observations on the Initial Report of South Africa, Human Rights Committee, UN Doc CCPR/C/ZAF/CO/1 (27 April 2016)

42. [The Committee] is also concerned about the wide scope of the data retention regime under the [2002 Regulation of Interception of Communications and Provision of Communication-Related Information Act]. [...]

43. The State Party should [...] consider revoking or limiting the requirement for mandatory retention of data by third parties. [...]

Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, UN Doc CCPR/C/USA/CO/4, (23 April 2014)

22. The State party should (d) "Refrain from imposing mandatory retention of data by third parties.

Commissioner for Human Rights, Council of Europe, Positions on Counter-Terrorism and Human Rights Protection, CommDH/PositionPaper(2015)1 (5 June 2015)

Independent ex ante authorisation should be extended to: untargeted bulk collection of information; the collection of and access to communications data (including when held by the private sector); and, potentially, computer network exploitation. The process by which intrusive measures are authorised or re-authorised should itself be subject to scrutiny. Given the difficulties that may arise when seeking to evaluate judicial decisions on the authorisation of intrusive measures, consideration may be given to quasi-judicial models.

***Szabó and Vissy v Hungary*, App No 37138/14, Judgment, European Court of Human Rights (12 January 2016)**

68. For the Court, it is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents. The techniques applied in such monitoring operations have demonstrated a remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen, especially when automated and systemic data collection is technically possible and becomes widespread. In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights. These data often compile further information about the conditions in which the primary elements intercepted by the authorities were created, such as the time and place of, as well as the equipment used for, the creation of computer files, digital photographs, electronic and text messages and the like. Indeed, it wouldde fy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European Union and, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities' enhanced technical possibilities to intercept private information.

69. The Court recalls that in Kennedy, the impugned legislation did not allow for "indiscriminate capturing of vast amounts of communications" which was one of the elements enabling it not to find a violation of Article 8. However, in the present case, the Court considers that, in the absence of specific rules to that effect or any submissions to the contrary, it cannot be ruled out that the broad-based provisions of the National Security Act can be taken to enable so-called strategic, large-scale interception, which is a matter of serious concern.

***S. and Marper v The United Kingdom*, Apps Nos 30562/04 and 30566/04, Judgment, European Court of Human Rights (4 December 2008)**

119. In this respect, the Court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken – and retained – from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time-limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database or the materials destroyed; in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances.

***Weber and Saravia v Germany*, App No 54934/00, Decision, European Court of Human Rights (29 June 2006)**

106. […] in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.

115. While the range of subjects in the amended G 10 Act is very broadly defined, the Court observes that... a series of restrictive conditions had to be satisfied before a measure entailing strategic monitoring could be imposed. It was merely in respect of certain serious criminal acts – which reflect threats with which society is confronted nowadays and which were listed in detail in the impugned section 3(1) – that permission for strategic monitoring could be sought.

***Spetsializirana prokuratura* (C-350/21), Judgment, Court of Justice of the European Union (17 November 2022) (translated from the original French)**

50. In that regard, even the storage of a limited amount of traffic data or location data or the storage of such data for a short period is likely to provide very precise information about the private life of a user of a means of electronic communication. Moreover, the quantity of the data available and the very precise information on the private life of the data subject resulting therefrom can be assessed only after consultation of that data. However, the interference resulting from the storage of that data necessarily occurs before the data and the resulting information can be consulted. Thus, the assessment of the seriousness of the interference constituted by the storage is necessarily made in the light of the risk generally associated with the category of data stored for the private life of the data subjects, regardless, moreover, of whether or not the information relating to private life derived therefrom is of a sensitive nature (Case C-793/19 and C-794/19 *SpaceNet and Telekom Deutschland* [2007] ECR I-0000, paragraph 89).

51. Thus, in the case giving rise to the judgment of 20 September 2022, C-793/19 and C-794/19 (*SpaceNet*, EU:C:2022: 702), the Court held that a set of traffic data and location data stored for the periods at issue in that case, namely ten weeks and four weeks respectively, could allow very precise conclusions to be drawn about the private lives of the persons whose data are stored, such as habits of daily life, permanent or temporary places of residence, daily or other movements, activities pursued, social relations of those persons and the social circles frequented by them, and thus to establish a profile of those persons (see, to that effect, judgment of 20 September 2022, *SpaceNet and Telekom Deutschland*, C-793/19 and C-794/19, EU: C:2022:702, paragraph 90).

52. The same applies a fortiori to a general and undifferentiated retention of traffic data and location data for a longer period, such as the six-month period at issue in the main proceedings.

***Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH* (C 793/19 and C 794/19), Judgment, Grand Chamber, Court of Justice of the European Union (20 September 2022)**

47. By its question, the referring court seeks, in essence, to ascertain whether Article 15(1) of Directive 2002/58, read in the light of Articles 6 to 8 and 11 and Article 52(l) of the Charter and Article 4(2) TEU, must be interpreted as meaning that it precludes a national legislative measure which, with certain exceptions, requires providers of publicly available electronic communications services – for the purposes set out in Article 15(1) of that directive, and inter alia for the purposes of prosecuting serious criminal offences or preventing a specific risk to national security – to retain, in a general and indiscriminate way, most of the traffic and location data of the end users of those services, laying down a retention period of several weeks and rules intended to ensure the effective protection of the retained data against the risks of abuse and against any unlawful access to those data.

51. As regards the system established by that directive of which Article 15(1) forms part, it must be recalled that, pursuant to the first and second sentences of Article 5(1) of that directive, Member States are required to ensure, through their national legislation, the confidentiality of communications by means of a public communications network and publicly available electronic communications services, as well as of the related traffic data. In particular, they are required to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1) of the same directive (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 34).

52. In that regard, the Court has already held that Article 5(1) of Directive 2002/58 enshrines the principle of confidentiality of both electronic communications and the related traffic data and requires inter alia that, in principle, persons other than users be prohibited from storing, without those users' consent, those communications and data (judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 107, and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 35).

53. That provision reflects the objective pursued by the EU legislature when adopting Directive 2002/58. It is apparent from the Explanatory Memorandum of the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000) 385 final), which gave rise to Directive 2002/58, that the EU legislature sought to 'ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used'. As is apparent from, inter alia, recitals 6 and 7 thereof, the purpose of that directive is to protect users of electronic communications services from risks for their personal data and privacy resulting from new technologies and, in particular, from the increasing capacity for automated storage and processing of data. In particular, as stated in recital 2 of the directive, the EU legislature's intent is to ensure full respect for the rights set out in Articles 7 and 8

of the Charter, relating, respectively, to respect for private and family life and the protection of personal data (see, to that effect, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 36 and the case-law cited).

55 As regards the processing and storage by electronic communications service providers of subscribers' and users' traffic data, Article 6 of Directive 2002/58 provides, in paragraph 1, that those data must be erased or made anonymous, when they are no longer needed for the purpose of the transmission of a communication, and states, in paragraph 2, that the traffic data necessary for the purposes of subscriber billing and interconnection fees may only be processed up to the end of the period during which the bill may lawfully be challenged or payment pursued. As regards location data other than traffic data, Article 9(1) of that directive provides that those data may be processed only subject to certain conditions and after they have been made anonymous or the consent of the users or subscribers obtained.

57. In so far as Article 15(1) of Directive 2002/58 permits Member States to adopt legislative measures that 'restrict the scope' of the rights and obligations laid down inter alia in Articles 5, 6 and 9 of that directive, such as those arising from the principles of confidentiality of communications and the prohibition on storing related data recalled in paragraph 52 above, that provision provides for an exception to the general rule provided for inter alia in Articles 5, 6 and 9 and must thus, in accordance with settled case-law, be the subject of a strict interpretation. That provision, therefore, cannot permit the exception to the obligation of principle to ensure the confidentiality of electronic communications and data relating thereto and, in particular, to the prohibition on storage of those data, laid down in Article 5 of that directive, to become the rule, if the latter provision is not to be rendered largely meaningless (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 40 and the case-law cited).

60. It should be made clear, in that regard, that the retention of traffic and location data constitutes, in itself, first, a derogation from the prohibition laid down in Article 5(1) of Directive 2002/58 barring any person other than the users from storing those data, and, secondly, an interference with the fundamental rights to the respect for private life and the protection of personal data, enshrined in Articles 7 and 8 of the Charter, irrespective of whether the information in question relating to private life is sensitive, whether the persons concerned have been inconvenienced in any way on account of that interference, or, furthermore, whether the data retained will or will not be used subsequently (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 44 and the case-law cited).

61. That conclusion is all the more justified since traffic and location data may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health, given that such data moreover enjoy special protection under EU law. Taken as a whole, those data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data have been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, those data provide the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 45 and the case-law cited).

62. Therefore, first, the retention of traffic and location data for policing purposes is liable, in itself, to infringe the right to respect for communications, enshrined in Article 7 of the Charter, and to deter users of electronic communications systems from exercising their freedom of expression, guaranteed in Article 11 of the Charter, effects that are all the more serious given the quantity and breadth of data retained. Secondly, in view of the significant quantity of traffic and location data that may be continuously retained under a general and indiscriminate retention measure, as well as the

sensitive nature of the information that may be gleaned from those data, the mere retention of such data by providers of electronic communications services entails a risk of abuse and unlawful access (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 46 and the case-law cited).

85. In the second place, as regards the data retention period, it follows from the second sentence of Article 15(1) of Directive 2002/58 that the length of the retention period provided for by a national measure imposing a general and indiscriminate retention obligation is indeed a relevant factor, amongst others, in determining whether EU law precludes such a measure, since that sentence requires that that period be 'limited'.

86. In the present case, it is true that those periods – which amount, according to Paragraph 113b(1) of the TKG, to 4 weeks for location data and to 10 weeks for other data – are significantly shorter that those provided for by the national legislation imposing a general and indiscriminate retention obligation examined by the Court in its judgments of 21 December 2016, Tele2 Sverige and Watson and Others (C-203/15 and C-698/15, EU:C:2016:970), of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), and of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, EU:C:2022:258).

87. However, as is apparent from the case-law cited in paragraph 61 above, the seriousness of the interference stems from the risk, particularly in view of their number and variety, that the data retained, taken as a whole, may enable very precise conclusions to be drawn concerning the private life of the person or persons whose data have been retained and, in particular, provide the means of establishing a profile of the person or persons concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.

88. Accordingly, the retention of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses, is in any event serious regardless of the length of the retention period and the quantity or nature of the data retained, when that set of data is liable to allow precise conclusions to be drawn concerning the private life of the person or persons concerned (see, as regards access to such data, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 39).

89. Even the retention of a limited quantity of traffic or location data or the retention of those data for a short period are liable to provide very precise information on the private life of a user of a means of electronic communication. Furthermore, the quantity of the data available and the very specific information on the private life of the person concerned that results from the data can be assessed only after the data have been consulted. However, the interference resulting from the retention of those data necessarily occurs before the data and the information resulting therefrom can be consulted. Thus, the assessment of the seriousness of the interference that the retention constitutes is necessarily carried out on the basis of the risk generally pertaining to the category of data retained for the private lives of the persons concerned, without it indeed mattering whether or not the resulting information relating to the person's private life is in actual fact sensitive (see, to that effect, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 40).

90. In the present case, as is apparent from paragraph 77 above and as was confirmed at the hearing, a set of traffic and location data retained for 10 weeks and 4 weeks respectively may allow very precise conclusions to be drawn concerning the private lives of the persons whose data are retained, such as habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them and, in particular, enable a profile of those persons to be established.

91. In the third place, as regards the safeguards provided for by the national legislation at issue in the main proceedings, which are intended to protect the retained data against the risks of abuse and against any unlawful access, it must be emphasised that the retention of and access to those data each constitute, as is clear from the case-law recalled in paragraph 60 above, separate interferences with the fundamental rights guaranteed by Articles 7 and 11 of the Charter, requiring a separate justification pursuant to Article 52(1) of the Charter. It follows that national legislation ensuring full respect for the conditions established by the case-law interpreting Directive 2002/58 as regards access to retained data cannot, by its very nature, be capable of either limiting or even remedying the serious interference, which results from the general retention of those data provided for under that national legislation, with the rights guaranteed by Articles 5 and 6 of that directive and by the fundamental rights to which those articles give specific effect (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 47).

101 It follows from all the foregoing that Article 47 of the Charter does not preclude a national court, when it rules on an application for authorisation of enforcement of the collection of biometric and genetic data of an accused person in order for them to be entered in a record, from being unable to assess the evidence on which the accusation of that person is based, provided that national law subsequently guarantees effective judicial review of the conditions for that accusation, from which the authorisation to collect those data arises.

107. The fact that the court which must make such a judicial decision cannot assess, at that stage of the criminal procedure, whether the evidence on which the accusation of the person concerned is based is sufficient constitutes a guarantee for the latter of observance of the right to be presumed innocent.

108. Such a guarantee is all the more necessary where national law, such as the provision at issue in the main proceedings, provides that the court having jurisdiction to rule on enforcement of collection of the biometric and genetic data concerning accused persons in order for them to be entered in a record is the court which, at the judicial stage of the criminal procedure, will have to rule on the criminal liability of such a person. Observance of the right to be presumed innocent requires that court to be free of any bias and any prejudice when it carries out that examination (see, to that effect, judgment of 16 November 2021, *Prokuratura Rejonowa w Mińsku Mazowieckim and Others*, C-748/19 to C-754/19, EU:C:2021:931, paragraph 88).

109. It should be borne in mind that, according to that case-law, the competent national authorities may adopt, for areas referred to in the preceding paragraph, a targeted measure of retention using a geographic criterion, such as, inter alia, the average crime rate in a geographical area, without that authority necessarily having specific indications as to the preparation or commission, in the areas concerned, of acts of serious crime. Since a targeted retention using that criterion is likely to concern, depending on the serious criminal offences in question and the situation specific to the respective Member States, both the areas marked by a high incidence of serious crime and areas particularly vulnerable to the commission of those acts, it is, in principle, not likely moreover to give rise to discrimination, as the criterion drawn from the average rate of serious crime is, in itself, entirely unconnected with any potentially discriminatory factors (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 80).

110. In addition and above all, a targeted measure of retention covering places or infrastructures which regularly receive a very high volume of visitors, or strategic places, such as airports, stations, maritime ports or tollbooth areas, allows the competent authorities to collect traffic data and, in particular, location data of all persons using, at a specific time, a means of electronic communication in one of those places. Thus, such a targeted retention measure may allow those authorities to obtain, through access to the retained data, information as to the presence of those persons in the places or geographical areas covered by that measure as well as their movements between or within those areas and to draw, for the purposes of combating serious crime, conclusions as to their

presence and activity in those places or geographical areas at a specific time during the period of retention (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 81).
127 It should be observed, first of all, that authorising access, for the purpose of combating serious crime, to traffic and location data which have been retained in a general and indiscriminate way would make that access depend upon circumstances unrelated to that objective, according to whether or not, in the Member State concerned, there was a serious threat to national security as referred to in the preceding paragraph, whereas, in view of the sole objective of the fight against serious crime which must justify the retention of those data and access thereto, there is nothing to justify a difference in treatment, in particular as between the Member States (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 97).

128 As the Court has already held, access to traffic and location data retained by providers of electronic communications services in accordance with a measure taken under Article 15(1) of Directive 2002/58, which must be given effect in full compliance with the conditions resulting from the case-law interpreting that directive, may, in principle, be justified only by the public interest objective for which those providers were ordered to retain those data. It is otherwise only if the importance of the objective pursued by access is greater than that of the objective which justified retention (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 98).

129 The Danish Government's argument refers to a situation in which the objective pursued by the access request proposed, namely the fight against serious crime, is of lesser importance in the hierarchy of objectives of public interest than that which justified the retention, namely the safeguarding of national security. To authorise, in that situation, access to retained data would be contrary to that hierarchy of public interest objectives recalled in the preceding paragraph and in paragraphs 68, 71, 72 and 73 above (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 99).

130 In addition and moreover, in accordance with the case-law recalled in paragraph 74 above, traffic and location data cannot be the object of general and indiscriminate retention for the purpose of combating serious crime and, therefore, access to those data cannot be justified for that same purpose. Where those data have exceptionally been retained in a general and indiscriminate way for the purpose of safeguarding national security against a genuine and present or foreseeable threat, in the circumstances referred to in paragraph 71 above, the national authorities competent to undertake criminal investigations cannot access those data in the context of criminal proceedings, without depriving of any effectiveness the prohibition on such retention for the purpose of combating serious crime, recalled in paragraph 74 above (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 100).

***Ligue des droits humains v Conseil des ministres* (C-817/19), Judgment, Grand Chamber, Court of Justice of the European Union (21 June 2022)**

110. Given how common use of air transport services is, the effect of a retention period that long is that a very large part of the population of the European Union is liable to have its PNR data retained, repeatedly, under the system established by the PNR Directive and, accordingly, be accessible for analyses carried out in the context of advance and subsequent assessments by the PIU and competent authorities over a considerable – even indefinite – period of time, in the case of persons who travel by air more than once every five years.

111. In the light of all of the foregoing, it is appropriate to find that the PNR Directive entails undeniably serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter, in so far, inter alia, as it seeks to introduce a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air transport services.

118. Thus, legislation that provides for the retention of personal data must continue to satisfy objective criteria that establish a connection between the data to be retained and the objective pursued (see, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 191 and the case-law cited, and judgments of 3 October 2019, A and Others, C-70/18, EU:C:2019:823, paragraph 63, and of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 133).

***G.D. v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, and Attorney General*, (C-140/20), Judgment, Grand Chamber, Court of Justice of the European Union (5 April 2022)**

31. By its first, second and fourth question, which it is appropriate to examine together, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that provides for the general and indiscriminate retention of traffic and location data for the purposes of combating serious crime.

32. It should be noted, as a preliminary point, that it is settled case-law that, in interpreting a provision of EU law, it is necessary not only to refer to its wording but also to consider its context and the objectives of the legislation of which it forms part, and in particular the origin of that legislation (judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 105 and the case-law cited).

33. It is clear from the wording itself of Article 15(1) of Directive 2002/58 that the legislative measures that it authorises Member States to take, under the conditions that it lays down, may seek only 'to restrict the scope' of the rights and obligations laid down inter alia in Articles 5, 6 and 9 of Directive 2002/58.

34. As regards the system established by that directive of which Article 15(1) forms part, it must be recalled that, pursuant to the first and second sentences of Article 5(1) of that directive, Member States are required to ensure, through their national legislation, the confidentiality of communications by means of a public communications network and publicly available electronic communications services, as well as of the related traffic data. In particular, they are required to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1) of the same directive.

35. In that regard, the Court has already held that Article 5(1) of Directive 2002/58 enshrines the principle of confidentiality of both electronic communications and the related traffic data and requires inter alia that, in principle, persons other than users be prohibited from storing, without those users' consent, those communications and data (judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 107).

36. That provision reflects the objective pursued by the EU legislature when adopting Directive 2002/58. It is apparent from the Explanatory Memorandum of the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000) 385 final), which gave rise to Directive 2002/58, that the EU legislature sought to 'ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used'. As is apparent from, inter alia, recitals 6 and 7 thereof, the purpose of that directive is to protect users of electronic communications services from risks for their personal data and privacy resulting from new technologies and, in particular, from the increasing capacity for automated storage and processing of data. In particular, as stated in recital 2 of the directive, the EU legislature's intent is to ensure full respect for the rights set out in Articles 7 and 8

of the Charter (see, to that effect, judgments of 21 December 2016, Tele2 Sverige and Watson and Others, C-203/15 and C-698/15, EU:C:2016:970, paragraph 83, and of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 106).

37. In adopting Directive 2002/58, the EU legislature gave concrete expression to those rights, so that the users of electronic communications services are entitled to expect, in principle, that their communications and data relating thereto will remain anonymous and may not be recorded, unless they have agreed otherwise (judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 109).

38. As regards the processing and storage by electronic communications service providers of subscribers' and users' traffic data, Article 6 of Directive 2002/58 provides, in paragraph 1, that those data must be erased or made anonymous when they are no longer needed for the purpose of the transmission of a communication, and states, in paragraph 2, that the traffic data necessary for the purposes of subscriber billing and interconnection fees may only be processed up to the end of the period during which the bill may lawfully be challenged or payments pursued in order to obtain payment. As regards location data other than traffic data, Article 9(1) of that directive provides that those data may be processed only subject to certain conditions and after they have been made anonymous or the consent of the users or subscribers obtained.

39. Therefore, Directive 2002/58 does not merely create a framework for access to such data through safeguards to prevent abuse, but also enshrines, in particular, the principle of the prohibition of their storage by third parties.

40. In so far as Article 15(1) of Directive 2002/58 permits Member States to adopt legislative measures that 'restrict the scope' of the rights and obligations laid down inter alia in Articles 5, 6 and 9 of that directive, such as those arising from the principles of confidentiality of communications and the prohibition on storing related data recalled in paragraph 35 of this judgment, that provision provides for an exception to the general rule provided for inter alia in Articles 5, 6 and 9 and must thus, in accordance with settled case-law, be the subject of a strict interpretation. That provision, therefore, cannot permit the exception to the obligation of principle to ensure the confidentiality of electronic communications and data relating thereto and, in particular, to the prohibition on storage of that data, laid down in Article 5 of that directive, to become the rule, if the latter provision is not to be rendered largely meaningless (see, to that effect, judgments of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 89, and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 111).

44. It should be made clear, in that regard, that the retention of traffic and location data constitutes, in itself, first, a derogation from the prohibition laid down in Article 5(1) of Directive 2002/58 barring any person other than the users from storing those data, and, second, an interference with the fundamental rights to the respect for private life and the protection of personal data, enshrined in Articles 7 and 8 of the Charter, irrespective of whether the information in question relating to private life is sensitive, whether the persons concerned have been inconvenienced in any way on account of that interference, or, furthermore, whether the data retained will or will not be used subsequently (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 115 and 116 and the case-law cited).

45. That conclusion is all the more justified since traffic and location data may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health, given that such data moreover enjoy special protection under EU law. Taken as a whole, those data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data have been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social

relationships of those persons and the social environments frequented by them. In particular, those data provide the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications (judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 117 and the case-law cited).

46. Therefore, first, the retention of traffic and location data for policing purposes is liable, in itself, to infringe the right to respect for communications, enshrined in Article 7 of the Charter, and to deter users of electronic communications systems from exercising their freedom of expression, guaranteed in Article 11 of the Charter, effects that are all the more serious given the quantity and breadth of data retained. Second, in view of the significant quantity of traffic and location data that may be continuously retained under a general and indiscriminate retention measure, as well as the sensitive nature of the information that may be gleaned from those data, the mere retention of such data by providers of electronic communications services entails a risk of abuse and unlawful access (see, to that effect, judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 118 and 119 and the case-law cited).

47. In that regard, it must be emphasised that the retention of and access to those data each constitute, as is clear from the case-law recalled in paragraph 44 of this judgment, separate interferences with the fundamental rights guaranteed by Articles 7 and 11 of the Charter, requiring a separate justification pursuant to Article 52(1) of the Charter. It follows that national legislation ensuring full respect for the conditions established by the case-law interpreting Directive 2002/58 as regards access to retained data cannot, by its very nature, be capable of either limiting or even remedying the serious interference, which results from the general retention of those data provided for under that national legislation, with the rights guaranteed by Articles 5 and 6 of that directive and by the fundamental rights to which those articles give specific effect.

83. As regards the possibility of providing distinctive criteria other than a personal or geographic criterion for the targeted retention of traffic and location data, it is possible that other objective and non-discriminatory criteria may be considered in order to ensure that the scope of a targeted retention measure is as limited as is strictly necessary and to establish a connection, at least indirectly, between serious criminal acts and the persons whose data are retained. However, since Article 15(1) of Directive 2002/58 refers to legislative measures of the Member States, it is for the latter and not for the Court to identify those criteria, it being understood that there can be no question of reinstating, by that means, the general and indiscriminate retention of traffic and location data.

84. In any event, as Advocate General Campos Sánchez-Bordona observed in point 50 of his Opinion in Joined Cases *SpaceNet and Telekom Deutschland* (C-793/19 and C-794/19, EU:C:2021:939), the fact that it may be difficult to provide a detailed definition of the circumstances and conditions under which targeted retention may be carried out is no reason for the Member States, by turning the exception into a rule, to provide for the general retention of traffic and location data.

85. As regards, second, the expedited retention of traffic and location data processed and stored by providers of electronic communications services on the basis of Articles 5, 6 and 9 of Directive 2002/58 or on the basis of legislative measures taken under Article 15(1) of that directive, it should be noted that those data must, in principle, be erased or made anonymous, depending on the circumstances, at the end of the statutory periods within which those data must be processed and stored in accordance with the national provisions transposing that directive. Nevertheless, the Court has held that during that processing and storage, situations may arise in which it becomes necessary to retain those data after those time periods have ended in order to shed light on serious criminal offences or acts adversely affecting national security; this is the case both in situations where those offences or acts having adverse effects have already been established and where, after an objective examination of all of the relevant circumstances, such offences or acts having adverse effects may

reasonably be suspected (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 160 and 161).

86. In such a situation, in the light of the balance that must be struck between the rights and interests at issue referred to in paragraphs 50 to 53 of this judgment, it is permissible for Member States to provide, in legislation adopted pursuant to Article 15(1) of Directive 2002/58, for the possibility of instructing, by means of a decision of the competent authority subject to effective judicial review, providers of electronic communications services to undertake the expedited retention of traffic and location data at their disposal for a specified period of time (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 163).

87. To the extent that the purpose of that expedited retention no longer corresponds to the purpose for which those data were initially collected and retained and since any processing of data must, under Article 8(2) of the Charter, be consistent with specified purposes, Member States must make clear, in their legislation, for what purpose the expedited retention of data may occur. In the light of the serious nature of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter which such retention may entail, only actions to combat serious crime and, a fortiori, to safeguard national security are such as to justify such interference, on the condition that the measure and access to the retained data comply with the limits of what is strictly necessary, as set out in paragraphs 164 to 167 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791).

88. The Court has stated that a measure of retention of that nature need not be limited to the data of persons who have been identified previously as being a threat to public security or national security of the Member State concerned or of persons specifically suspected of having committed a serious criminal offence or acts adversely affecting national security. According to the Court, while it must comply with the framework established by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, and taking into account the findings in paragraph 55 of this judgment, such a measure may, at the choice of the national legislature and subject to the limits of what is strictly necessary, be extended to traffic and location data relating to persons other than those who are suspected of having planned or committed a serious criminal offence or acts adversely affecting national security, provided that those data can, on the basis of objective and non-discriminatory factors, shed light on such an offence or acts adversely affecting national security, such as data concerning the victim thereof, and his or her social or professional circle (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 165).

89. Thus, a legislative measure may authorise the issuing of an instruction to providers of electronic communications services to carry out the expedited retention of traffic and location data, inter alia, of persons with whom, prior to the serious threat to public security arising or a serious crime being committed, a victim was in contact via those electronic means of communications.

90. Such expedited retention may, according to the Court's case-law recalled in paragraph 88 of this judgment and under the same conditions as those referred to in that paragraph, also be extended to specific geographic areas, such as the places of the commission of or preparation for the offence or attack on national security in question. It should be stated that the subject matter of such a measure may also be the traffic and location data relating to a place or a person, possibly the victim of a serious crime, who has disappeared, on condition that that measure and access to the data so retained comply with the limits of what is strictly necessary, as set out in paragraphs 164 to 167 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791).

91. Furthermore, it must be stated that Article 15(1) of Directive 2002/58 does not preclude the competent national authorities from ordering a measure of expedited retention at the first stage of an investigation into a serious threat for public security or a possible serious crime, namely from the

time when the authorities may, in accordance with the provisions of national law, commence such an investigation.

92. As regards the variety of measures for the retention of traffic and location data referred to in paragraph 67 of this judgment, it must be stated that those various measures may, at the choice of the national legislature and subject to the limits of what is strictly necessary, be applied concurrently. Accordingly, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as interpreted by case-law resulting from the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), does not preclude a combination of those measures.

***Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service (C-623/17)*, Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2020)**

51. […] section 94 of the 1984 Act permits the Secretary of State to require providers of electronic communications services, by way of directions, if he considers it necessary in the interests of national security or relations with a foreign government, to forward bulk communications data to the security and intelligence agencies. That data includes traffic data and location data, as well as information relating to the services used, pursuant to section 21(4) and (6) of the RIPA. That provision covers, inter alia, the data necessary to (i) identify the source and destination of a communication, (ii) determine the date, time, length and type of communication, (iii) identify the hardware used, and (iv) locate the terminal equipment and the communications. That data includes, inter alia, the name and address of the user, the telephone number of the person making the call and the number called by that person, the IP addresses of the source and addressee of the communication and the addresses of the websites visited.

52. Such a disclosure of data by transmission concerns all users of means of electronic communication, without its being specified whether that transmission must take place in real-time or subsequently. Once transmitted, that data is, according to the information set out in the request for a preliminary ruling, retained by the security and intelligence agencies and remains available to those agencies for the purposes of their activities, as with the other databases maintained by those agencies. In particular, the data thus acquired, which is subject to bulk automated processing and analysis, may be cross-checked with other databases containing different categories of bulk personal data or be disclosed outside those agencies and to third countries. Lastly, those operations do not require prior authorisation from a court or independent administrative authority and do not involve notifying the persons concerned in any way.

***La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées; Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministers (C-511/18, C-512/18 and C-520/18)*, Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2020)**

168. […] Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding legislative measures which, for the purposes laid down in Article 15(1), provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data. By contrast, Article 15(1), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not preclude legislative measures that:

- allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable,

where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists;

- provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;
- provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of IP addresses assigned to the source of an Internet connection for a period that is limited in time to what is strictly necessary;
- provide, for the purposes of safeguarding national security, combating crime and safeguarding public security, for the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems;
- allow, for the purposes of combating serious crime and, a fortiori, safeguarding national security, recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,

provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse."

***Tele2 Sverige AB v Post- Och telestyrelsen* (C-203/15); *Secretary of State for the Home Department v Tom Watson et. al.* (C-698/16), Joined Cases, Judgment, Grand Chamber, Court of Justice of the European Union (21 December 2016)**

77. The protection of the confidentiality of electronic communications and related traffic data, guaranteed in Article 5(1) of Directive 2002/58, applies to the measures taken by all persons other than users, whether private persons or bodies or State bodies. […]

85. The principle of confidentiality of communications established by Directive 2002/58 implies, inter alia, as stated in the second sentence of Article 5(1) of that directive, that, as a general rule, any person other than the users is prohibited from storing, without the consent of the users concerned, the traffic data related to electronic communications. The only exceptions relate to persons lawfully authorised in accordance with Article 15(1) of that directive and to the technical storage necessary for conveyance of a communication [...]

86. Accordingly, as confirmed by recitals 22 and 26 of Directive 2002/58, under Article 6 of that directive, the processing and storage of traffic data are permitted only to the extent necessary and for the time necessary for the billing and marketing of services and the provision of value added services. As regards, in particular, the billing of services, that processing is permitted only up to the end of the period during which the bill may be lawfully challenged or legal proceedings brought to obtain payment. Once that period has elapsed, the data processed and stored must be erased or made anonymous. As regards location data other than traffic data, Article 9(1) of that directive provides that that data may be processed only subject to certain conditions and after it has been made anonymous or the consent of the users or subscribers obtained.

87. The scope of Article 5, Article 6 and Article 9(1) of Directive 2002/58, which seek to ensure the confidentiality of communications and related data, and to minimise the risks of misuse, must moreover be assessed in the light of recital 30 of that directive, which states: 'Systems for the

provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum'. […]

103. […] while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight. […]

105. National legislation such as that at issue in the main proceedings, which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy. […]

109. In order to satisfy the requirements set out in the preceding paragraph of the present Judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary.

110. Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.

111. As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences. […]

122. With respect to the rules relating to the security and protection of data retained by providers of electronic communications services [...] providers [are required] to take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period.

***Digital Rights Ireland Ltd Minister of Communications, Marine and Natural Resources et al*. (C-293/12); *Kärntner Landesregierung and other*s (C-594/12), Joined Cases, Judgment, Grand Chamber, Court of Justice of the European Union (8 April 2014)**

39. So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.

40. Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data. […]

49. As regards the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive.

50. […] Whilst, admittedly, that fact is such as to limit the ability of the data retention measure to attain the objective pursued, it is not, however, such as to make that measure inappropriate, as the Advocate General has pointed out in paragraph 137 of his Opinion.

54. Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data.

55. The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data.

56. As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.

57. In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

58. Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

59. Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

60. Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.

61. Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.

62. In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.

63. Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

64. Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.

65. It follows from the above that Directive 2006/24 does not lay down clear and precise rules

governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

66. Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.

67. Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.

SECTION 6: SURVEILLANCE-RELATED CAPABILITIES

A. ENCRYPTION AND "GOING DARK"

The review of pronouncements by different human rights monitoring mechanisms shows that there are significant overlaps in references to encryption, the protection of journalists and human rights defenders. For this reason, it may be helpful to consult the content of all the relevant sub-chapters.

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

Emphasizing that, in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity, are important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of opinion and expression and to freedom of peaceful assembly and association, and recognizing that States should refrain from employing unlawful or arbitrary surveillance techniques, which may include forms of hacking,

12. *Emphasizes* that, in the digital age, encryption and anonymity tools have become vital for many journalists and media workers to freely exercise their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources, and calls upon States not to interfere with the use by journalists and media workers of such technologies and to ensure that any restrictions thereon comply with the obligations of States under international human rights law;

** See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018)*

UN General Assembly Resolution on the Safety of journalists and the issue of impunity, UN Doc A/RES/78/215 (19 December 2023)*

18. *Emphasizes* that, in the digital age, encryption and anonymity tools have become vital for many journalists to freely exercise their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources, and calls upon States not to interfere with the use of such technologies and to ensure that any restrictions thereon comply with States' obligations under international human rights law;

** See also UN General Assembly Resolution on the Safety of Journalists and the Issue of Impunity, UN Doc A/RES/74/157 (18 December 2019); UN General Assembly Resolution on the Safety of Journalists and the Issue of Impunity, UN Doc A/RES/72/175 (19 December 2017)*

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

Emphasizing that, in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity,

are important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of opinion and expression and to freedom of peaceful assembly and association, and recognizing that States must promote such measures and refrain from employing unlawful or arbitrary surveillance techniques, which may include forms of hacking and restrictions on accessing and using encryption technology,

12. *Encourages* business enterprises, including communications service providers, to work towards enabling solutions to secure and protect the confidentiality of digital communications and transactions, including measures for encryption, pseudonymization and anonymity, and to ensure the implementation of human-rights compliant safeguards, and calls upon States to promote measures and technical solutions for strong encryption, pseudonymization and anonymity, not to interfere with the use of such technical solutions, with any restrictions thereon complying with States' obligations under international human rights law, and to enact policies that protect the privacy of individuals' digital communications;

** See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021)*

UN Human Rights Council Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, UN Doc A/HRC/RES/47/16 (13 July 2021)*

Emphasizing that, in the digital age, technical solutions to secure and protect the confidentiality of digital communications, including measures for encryption and anonymity, are important to ensure the enjoyment of all human rights offline and online,

** See also UN Human Rights Council Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/RES/38/7 (5 July 2018)*

UN Human Rights Council Resolution on the Freedom of Opinion and Expression, UN Doc A/HRC/RES/44/12 (24 July 2020)

Underlining that digital contexts provide opportunities for exercising the right to freedom of opinion and expression, regardless of frontiers, for improving access to information and for seeking, receiving and imparting information and ideas of all kinds, and emphasizing that, in the digital age, technical solutions to secure and protect the confidentiality of digital communications, including measures for encryption and anonymity, can be important to ensure the enjoyment of human rights, including the right to freedom of opinion and expression,

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

20. In recent years, various Governments have taken actions, which, intentionally or not, risk undermining the security and confidentiality of encrypted communications. This has concerning implications for the enjoyment of the right to privacy and other human rights.

21. Encryption is a key enabler of privacy and security online and is essential for safeguarding rights, including the rights to freedom of opinion and expression, freedom of association and peaceful assembly, security, health and non-discrimination. […] In specific instances, journalists and human rights defenders cannot do their work without the protection of robust encryption, shielding their sources and sheltering them from the powerful actors under investigation. […]

24. […] Governments seeking to limit encryption have often failed to show that the restrictions they would impose are necessary to meet a particular legitimate interest, given the availability of various other tools and approaches that provide the information needed for specific law

enforcement or other legitimate purposes. Such alternative measures include improved, better-resourced traditional policing, undercover operations, metadata analysis and strengthened international police cooperation.

25. Moreover, the impact of most encryption restrictions on the right to privacy and associated rights are disproportionate, often affecting not only the targeted individuals but the general population. Outright bans by Governments, or the criminalization of encryption in particular, cannot be justified as they would prevent all users within their jurisdictions from having a secure way to communicate. Key escrow systems have significant vulnerabilities, since they depend on the integrity of the storage facility and expose stored keys to cyberattacks. Moreover, mandated back doors in encryption tools create liabilities that go far beyond their usefulness with regard to specific users identified as crime suspects or security threats. They jeopardize the privacy and security of all users and expose them to unlawful interference, not only by States, but also by non-State actors, including criminal networks. Licensing and registration requirements have similar disproportionate effects as they require that encryption software contain exploitable weaknesses. Such adverse effects are not necessarily limited to the jurisdiction imposing the restriction; rather it is likely that back doors, once established in the jurisdiction of one State, will become part of the software used in other parts of the world.

26. […] Client-side scanning moves the step of detection of content from the servers through which communications are sent to the personal devices themselves. In this way, content at issue is examined before being encrypted for transport. […] However, various legislative attempts may at least indirectly compel Internet communications services to implement such systems by imposing broad monitoring obligations for all communications, including those that are encrypted. […]

27. […] Unlike other interventions, mandating general client-side scanning would inevitably affect everyone using modern means of communication, not only people involved in crime and serious security threats. […] Given the possibility of such impacts, indiscriminate surveillance is likely to have a significant chilling effect on free expression and association, with people limiting the ways they communicate and interact with others and engaging in self-censorship.

28. […] where the rule of law is weak and human rights are under threat, the impact of client-side screening could be much broader, for example it could be used to suppress political debate or to target opposition figures, journalists and human rights defenders. Given the broad range of significant risks to human rights protection from mandated general client-side screening, such requirements should not be imposed without further substantial consideration of their potential human rights impacts and measures that mitigate those harms. Without in-depth investigation and analysis, it seems unlikely that such restrictions could be considered proportionate under international human rights law, even when imposed in pursuit of legitimate aims, given the severity of their possible consequences.

56. […] OHCHR recommends that States: (a) Ensure that any interference with the right to privacy, including hacking, restrictions to access and use of encryption technology and surveillance of the public, complies with international human rights law, including the principles of legality, legitimate aim, necessity and proportionality and non-discrimination, and does not impair the essence of that right;

57. […] OHCHR recommends that States: (b) Promote and protect strong encryption and avoid all direct, or indirect, general and indiscriminate restrictions on the use of encryption, such as prohibitions, criminalization, the imposition of weak encryption standards or requirements for mandatory general client-side scanning; interference with the encryption of private communications of individuals should only be carried out when authorized by an independent judiciary body and on a case-by-case basis, targeting individuals if strictly necessary for the

investigation of serious crimes or the prevention of serious crimes or serious threats to public safety or national security;

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/29/32 (22 May 2015)

31. Restrictions on encryption and anonymity, as enablers of the right to freedom of expression, must meet the well-known three-part test: any limitation on expression must be provided for by law; may only be imposed for legitimate grounds (as set out in article 19 (3) of the Covenant); and must conform to the strict tests of necessity and proportionality.

32. First, for a restriction on encryption or anonymity to be "provided for by law", it must be precise, public and transparent, and avoid providing State authorities with unbounded discretion to apply the. Proposals to impose restrictions on encryption or anonymity should be subject to public comment and only be adopted, if at all, according to regular legislative process. Strong procedural and judicial safeguards should also be applied to guarantee the due process rights of any individual whose use of encryption or anonymity is subject to restriction. In particular, a court, tribunal or other independent adjudicatory body must supervise the application of the restriction.

33. Second, limitations may only be justified to protect specified interests: rights or reputations of others; national security; public order; public health or morals [...] No other grounds may justify restrictions on the freedom of expression. Moreover, because legitimate objectives are often cited as a pretext for illegitimate purposes, the restrictions themselves must be applied narrowly.

34. Third, the State must show that any restriction on encryption or anonymity is "necessary" to achieve the legitimate objective. The European Court of Human Rights has concluded appropriately that the word "necessary" in article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms means that the restriction must be something more than "useful," "reasonable" or "desirable". Once the legitimate objective has been achieved, the restriction may no longer be applied. Given the fundamental rights at issue, limitations should be subject to independent and impartial judicial authority, in particular to preserve the due process rights of individuals.

35. Necessity also implies an assessment of the proportionality of the measures limiting the use of and access to security online. A proportionality assessment should ensure that the restriction is "the least intrusive instrument amongst those which might achieve the desired result". The limitation must target a specific objective and not unduly intrude upon other rights of targeted persons, and the interference with third parties' rights must be limited and justified in the light of the interest supported by the intrusion. The restriction must also be "proportionate to the interest to be protected". A high risk of damage to a critical, legitimate State interest may justify limited intrusions on the freedom of expression. Conversely, where a restriction has a broad impact on individuals who pose no threat to a legitimate government interest, the State's burden to justify the restriction will be very high. Moreover, a proportionality analysis must take into account the strong possibility that encroachments on encryption and anonymity will be exploited by the same criminal and terrorist networks that the limitations aim to deter. In any case, "a detailed and evidence-based public justification" is critical to enable transparent public debate over restrictions that implicate and possibly undermine freedom of expression. [...]

45. In a situation where law enforcement or national security arguments may justify requests for access to communications, authorities may see two options: order either decryption of particular communications or, because of a lack of confidence that a targeted party would comply with a decryption order, disclosure of the key necessary for decryption. Targeted decryption orders may be seen as more limited and less likely to raise proportionality concerns than key disclosures, focusing on specific communications rather than an individual's entire set of communications

encrypted by a particular key. Key disclosures, by contrast, could expose private data well beyond what is required by the exigencies of a situation. Moreover, key disclosure or decryption orders often force corporations to cooperate with Governments, creating serious challenges that implicate individual users online. Key disclosures exist by law in a number of European countries. In both cases, however, such orders should be based on publicly accessible law, clearly limited in scope, focused on a specific target, implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets, and only adopted when necessary and when less intrusive means of investigation are not available. Such measures may only be justified if used in targeting a specific user or users, subject to judicial oversight.

59. States should promote strong encryption and anonymity. National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online. Legislation and regulations protecting human rights defenders and journalists should also include provisions enabling access and providing support to use the technologies to secure their communications.

60. States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression. Blanket prohibitions fail to be necessary and proportionate. States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows. In addition, States should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users. Corporate actors should likewise consider their own policies that restrict encryption and anonymity (including through the use of pseudonyms). Court-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals."

62. […] Companies, like States, should refrain from blocking or limiting the transmission of encrypted communications and permit anonymous communication. Attention should be given to efforts to expand the availability of encrypted data-centre links, support secure technologies for websites and develop widespread default end-to-end encryption. Corporate actors that supply technology to undermine encryption and anonymity should be especially transparent as to their products and customers."

African Commission on Human and Peoples' Rights, Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa, ACHPR/Res.573 (LXXVII) (9 November 2023)

The African Commission calls on States Parties to: iv. Promote and encourage the use of privacy-enhancing technologies and desist from adopting laws or other measures prohibiting or weakening encryption, including backdoors, key escrows and data localization requirements, unless such measures are justifiable and compatible with international human rights law and standards;

Annual Report of the Inter-American Commission on Human Rights 2020, Volume II – Annual Report of the Office of the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II Doc 28 (30 March 2021)

175. The privacy of information in the digital age must be preserved. To this end, states must protect anonymity, as well as the encryption and inviolability of communications. They must set limits on the power to monitor private communications and establish the necessity and proportionality of such surveillance in accordance with individual human rights and the principles

of international law. Provisions on the mandatory registration of SIM cards and cell phones and any other measure that could lead to intercepting communications outside the limits permitted by international law must also be legitimate and must not violate the confidentiality of sources.

Annual Report of the Inter-American Commission on Human Rights 2019, Volume II – Annual Report of the Special Rapporteur for Freedom of Expression, Guide to Guarantee Freedom of Expression Regarding Deliberate Disinformation in Electoral Contexts, October 2019, OEA/Ser.L/V/II. Doc 5 (24 February 2020)

Likewise, it must be borne in mind that state's responses to the phenomenon of misinformation must be concerned about not affecting the integrity of the computer systems on which the Internet works and the communications that are channeled through the network. Thus, for instance, the fact that it has been documented that at least part of the disinformation campaigns use encrypted messaging systems could never lead to questioning the end-to-end encryption of communications, which are essential to protect privacy – and consequently, freedom – of citizens' communications.

UN General Assembly Resolution on the Promotion and Protection of Human Right in the Context of Digital Technologies, UN Doc A/RES/78/213 (19 December 2023)

Emphasizing that, in the digital age, technical solutions to secure and to protect the confidentiality of digital communications and transactions, including measures for strong encryption, pseudonymization and anonymity, are important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of opinion and expression and to freedom of peaceful assembly and association, and recognizing that Member States should promote such measures and refrain from employing unlawful or arbitrary surveillance techniques, which may include forms of hacking,

15. *Urges* Member States to refrain from interference with the use of technologies such as encryption and anonymity tools, and from employing unlawful or arbitrary surveillance techniques, including through hacking;

17. *Emphasizes* that, in the digital age, encryption and anonymity tools have become vital for many journalists and media workers to freely exercise their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources, and calls upon States not to interfere with the use by journalists and media workers of such technologies and to ensure that any restrictions thereon comply with the obligations of States under international human rights law;

UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/51/9 (6 October 2022)*

Emphasizing the particular risks with regard to the safety of journalists in the digital age, including the particular vulnerability of journalists to becoming targets of unlawful or arbitrary surveillance and/or the interception of communications, hacking, including government-sponsored hacking, malware, spyware, forced data handover or denial of service attacks to force the shutdown of particular media websites or services, in violation of their rights to privacy and to freedom of expression,

Emphasizing also that, in the digital age, encryption, pseudonymization and anonymity tools have become vital for many journalists to exercise freely their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources,

11. *Calls upon* States: (l) To refrain from interference with the use of technologies such as encryption and anonymity tools, and from employing unlawful or arbitrary surveillance techniques, including through hacking;

** See also UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/45/18 (12 October 2020); UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/39/6 (27 September 2018); UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/33/2 (29 September 2016)*

UN Human Rights Council Resolution on the Promotion and protection of human rights in the context of peaceful protests, UN Doc A/HRC/RES/50/21 (8 July 2022)

Emphasizing that technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity online, are important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association,

32. *Calls upon* States to refrain from applying any undue restrictions to technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity online, given that these are important to ensure the enjoyment of human rights, in particular the rights to privacy, in the context of assemblies;

UN Human Rights Council Resolution on Freedom of Opinion and Expression, UN Doc A/HRC/RES/50/15 (8 July 2022)

11. *Encourages* business enterprises, including communications service providers, to work towards enabling solutions to secure and protect the confidentiality of digital communications and transactions, including measures for encryption, pseudonymization and anonymity, and to ensure the implementation of human rights-compliant safeguards, and calls upon States not to interfere with the use of such technical solutions with any restrictions thereon complying with States' obligations under international human rights law, and to enact policies that protect the privacy of individuals' digital communications;

UN Human Rights Council Resolution on The promotion and protection of human rights in the context of peaceful protests, UN Doc A/HRC/RES/50/21 (8 July 2022)

32. *Calls upon* States to refrain from applying any undue restrictions to technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity online, given that these are important to ensure the enjoyment of human rights, in particular the rights to privacy, in the context of assemblies;

Report of the United Nations High Commissioner for Human Rights, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests, UN Doc A/HRC/44/24 (24 June 2020)

8. […] Messaging and social networking platforms that use encryption technology to prevent monitoring enhance the security of civil society groups' digital communication, while also providing tools specifically geared to network organizing at the grass-roots level. To protect the safety of communications, some messaging platforms have adopted the use of end-to-end encryption.

13. […] Moreover, there are also responsibilities for the social media companies that control online spaces, particularly with regard to encryption, content moderation, and algorithmic amplification […].

24. Safe and confidential communications play a key role in the planning and holding of peaceful

protests. Technology-enabled surveillance poses significant risks to the enjoyment of human rights in peaceful assemblies and is an important contributor to the shrinking of civic space in many countries. […] In response to this trend, the Human Rights Council has underlined the importance of privacy online for the realization of the rights of peaceful assembly and association. It has also emphasized that technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption and anonymity, can be important to ensure the enjoyment of these rights. In her report on the right to privacy in the digital age, the High Commissioner outlined key safeguards that States should implement for surveillance measures. National legal frameworks, based on the principles of necessity and proportionality, are needed to regulate the use of surveillance tools.

25. Similarly, the Special Rapporteur on the right to freedom of opinion and expression has called for strict limitations on restrictions to encryption and anonymity in order to ensure compliance with the principles of legality, necessity, proportionality and legitimacy. Such restrictions are often used by law enforcement and intelligence agencies as quick reactions to terrorism, while failing to meet imperatives of necessity and proportionality, and consequently undermining trust in the rule of law. Other experts have recalled the importance of judicial control and proportionality when anonymity is lifted.

53. In this context, the High Commissioner recommends that States: (e) Promote and protect strong encryption and anonymity options online, and ensure that laws provide for judicial supervision for any lifting of anonymity;

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

20. […] Encryption and anonymity tools are widely used around the world, including by human rights defenders, civil society, journalists, whistle-blowers and political dissidents facing persecution and harassment. Weakening them jeopardizes the privacy of all users and exposes them to unlawful interferences not only by States, but also by non-State actors, including criminal networks. Such a widespread and indiscriminate impact is not compatible with the principle of proportionality (see A/HRC/29/32, para. 36).

Report of the Special Rapporteur on the Independence of Judges and Lawyers, 'Reimagining justice: confronting contemporary challenges to the independence of judges and lawyers', UN Doc A/HRC/53/31 (13 April 2023)

66. […] Encryption is a key enabler of privacy and security online, and it is essential for safeguarding rights, including the rights to freedom of opinion and expression, freedom of association and peaceful assembly. It ensures that individuals can share information freely, without fear that their information may become known to others, such as State authorities or cybercriminals. Encryption is essential if individuals are to feel secure in freely exchanging information, including financial information, with others. In specific instances, journalists and human rights defenders cannot do their work without the protection of robust encryption, shielding their sources and sheltering them from powerful actors. Encryption and anonymity tools can counter threats to privacy and allow users to exercise their rights to freedom of opinion and expression more safely. In parallel, national laws should be developed to ensure strong data protection, in line with human rights standards.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/75/261 (28 July 2020)

48. State assertions that national security or public order justifies interference with personal security and privacy are common in cases of surveillance of personal communications, encryption and anonymity. […]

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/43/52 (24 March 2020)

52. States and non-State actors should: (a) Protect the privacy of digital communications and enjoyment of the right to privacy by all individuals, regardless of their gender, by promoting tools such as encryption;

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, UN Doc A/HRC/41/41 (17 May 2019)

24. Encryption technologies, pseudonymity and other security features have enabled individuals belonging to minority groups to find one another and create community. The Human Rights Council has stressed that "technical solutions to secure and protect the confidentiality of digital communications, including measures for encryption and anonymity, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association". The Special Rapporteur asserts that the same is true for the organization and conduct of associations. These tools provide individuals and civil society actors with safe online space to gather and connect with other members of their group as well as to organize and coordinate activities, without undue interference from third parties and government.

61. Policies and features on user privacy and security of communications can also affect the enjoyment of the rights of peaceful assembly and association. Only a few digital technology companies allow the use of pseudonyms or other ways to mask an individual's identity, or provide for encrypted communications. […]

73. States should create an enabling legal framework for the right to peaceful assembly and association in the digital age, by: (d) Promoting and protecting strong encryption and anonymity, including by adopting laws, regulations and policies that confer only on courts the power to remove the right to anonymity, rather than on law enforcement agencies.

Report of the Special Rapporteur on the Situation of Human Rights Defenders, Situation of Women Human Rights Defenders, UN Doc A/HRC/40/60 (10 January 2019)

Priority 6: Recognize that security must be understood holistically and that it encompasses physical safety, digital security, environmental security, economic stability, the freedom to practice cultural and religious beliefs and the mental and emotional well-being of women defenders and their families and loved ones.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/23/40 (17 April 2013)

88. States should refrain from compelling the identification of users as a precondition for access to communications, including online services, cybercafés, or mobile telephony.

89. Individuals should be free to use whatever technology they choose to secure their communications. States should not interfere with the use of encryption technologies, nor compel the provision of encryption keys.

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet OEA/Ser.L/V/II. CIDH/RELE/INF.11/13 (31 December 2013)

150. As far as freedom of expression is concerned, the violation of the privacy of communications can give rise to a direct restriction when—for example—the right cannot be exercised anonymously as a consequence of the surveillance activity. In addition, the mere existence of these types of

programs leads to an indirect limitation that has a chilling effect on the exercise of freedom of expression. Indeed, the violation of the privacy of communications makes people cautious of what they say and—therefore—of what they do; it instils fear and inhibition as part of the political culture, and it forces individuals to take precautions in communicating with others. Moreover, the people most affected are those who take unpopular positions, or the members of political, racial, or religious minorities who are often unjustifiably classified as "terrorists," which makes them the object of surveillance and monitoring without proper oversight. A democratic society requires that individuals be able to communicate without undue interference, which means that their communications must be private and secure [...]

***Podchasov v Russia*, App No 33696/19, Judgment, European Court of Human Rights (13 February 2024)**

56. Lastly, as regards the ICOs' statutory obligation to decrypt communications if they are encrypted (see paragraphs 20 and 24 above), the Court observes that the parties' observations on this issue are limited to end-to-end encrypted communications, that is, in the case of Telegram, communications through "secret chats" (see paragraph 5 above). The parties did not make any submissions in respect of the encryption scheme used in "cloud chats" and the Court will therefore not examine it.

76. Lastly, as regards the requirement to submit to the security services information necessary to decrypt electronic communications if they are encrypted, the Court observes that international bodies have argued that encryption provides strong technical safeguards against unlawful access to the content of communications and has therefore been widely used as a means of protecting the right to respect for private life and for the privacy of correspondence online […]

77. As noted above (see paragraph 57 above), it appears that in order to enable decryption of communications protected by end-to-end encryption, such as communications through Telegram's "secret chats", it would be necessary to weaken encryption for all users. These measures allegedly cannot be limited to specific individuals and would affect everyone indiscriminately, including individuals who pose no threat to a legitimate government interest. Weakening encryption by creating backdoors would apparently make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications. Backdoors may also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications. The Court takes note of the dangers of restricting encryption described by many experts in the field (see, in particular, paragraphs 28 and 34 above).

78. The Court accepts that encryption can also be used by criminals, which may complicate criminal investigations (see *Yüksel Yalçınkaya v. Türkiye* [GC], no. 15669/20, § 312, 26 September 2023). However, it takes note in this connection of the calls for alternative "solutions to decryption without weakening the protective mechanisms, both in legislation and through continuous technical evolution" (see, on the possibilities of alternative methods of investigation, the Joint Statement by Europol and the European Union Agency for Cybersecurity, cited in paragraph 33 above, and paragraph 24 of the Report on the right to privacy in the digital age by the Office of the United Nations High Commissioner for Human Rights, cited in paragraph 28 above; see also the explanation by third-party interveners in paragraph 47 above).

79. The Court concludes that in the present case the ICO's statutory obligation to decrypt end-to-end encrypted communications risks amounting to a requirement that providers of such services weaken the encryption mechanism for all users; it is accordingly not proportionate to the legitimate aims pursued.

80. The Court concludes from the foregoing that the contested legislation providing for the retention of all Internet communications of all users, the security services' direct access to the data stored without adequate safeguards against abuse and the requirement to decrypt encrypted

communications, as applied to end-to-end encrypted communications, cannot be regarded as necessary in a democratic society. In so far as this legislation permits the public authorities to have access, on a generalised basis and without sufficient safeguards, to the content of electronic communications, it impairs the very essence of the right to respect for private life under Article 8 of the Convention. The respondent State has therefore overstepped any acceptable margin of appreciation in this regard.

B. THE DEBATE OVER HACKING, INCLUDING SPYWARE AND VULNERABILITY EXPLOITATION

The review of pronouncements by different human rights monitoring mechanisms shows that there are significant overlaps in references to encryption, the protection of journalists and human rights defenders. For this reason, it may be helpful to consult the content of all the relevant sub-chapters.

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

Emphasizing that, in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity, are important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of opinion and expression and to freedom of peaceful assembly and association, and recognizing that States should refrain from employing unlawful or arbitrary surveillance techniques, which may include forms of hacking,

** See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018)*

UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/51/9 (6 October 2022)*

Emphasizing the particular risks with regard to the safety of journalists in the digital age, including the particular vulnerability of journalists to becoming targets of unlawful or arbitrary surveillance and/or the interception of communications, hacking, including government-sponsored hacking, malware, spyware, forced data handover or denial of service attacks to force the shutdown of particular media websites or services, in violation of their rights to privacy and to freedom of expression,

11. *Calls upon* States: (l) To refrain from interference with the use of technologies such as encryption and anonymity tools, and from employing unlawful or arbitrary surveillance techniques, including through hacking;

** See also UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/45/18 (12 October 2020); UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/39/6 (27 September 2018); UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/33/2 (29 September 2016)*

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

Noting that the rapid pace of technological development enables individuals all over the world to

use information and communications technology, and at the same time enhances the capacity of Governments, business enterprises and individuals to undertake surveillance, interception, hacking and data collection, which may violate or abuse human rights, in particular the right to privacy, and is therefore an issue of increasing concern,

Noting with deep concern also the use of technological tools developed by the private surveillance industry by private or public actors to undertake surveillance, hacking of devices and systems, including through the use of malware or spyware, interception and disruption of communications, and data collection, interfering with the professional and private lives of individuals, including those engaged in the promotion and defence of human rights and fundamental freedoms, journalists and other media workers, in violation or abuse of their human rights, specifically the right to privacy,

Emphasizing that, in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity, are important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of opinion and expression and to freedom of peaceful assembly and association, and recognizing that States must promote such measures and refrain from employing unlawful or arbitrary surveillance techniques, which may include forms of hacking and restrictions on accessing and using encryption technology,

** See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019);*

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

9. The hacking of personal communication devices constitutes a serious interference with the right to privacy and can be linked to concerning violations of a range of other rights. […]

11. Hacking may also have a negative impact on the rights to due process and fair trial. Gaining access to a device can enable an intruder not only to observe the contents of that device and its interactions with other devices but also to manipulate the device, including by altering, deleting or adding files. It is thus possible to forge evidence in order to incriminate or blackmail targeted individuals.

16. […] The far-reaching adverse impacts of hacking require a particularly cautious approach to its use, limiting it to the most exceptional circumstances, in strict adherence with the requirements of international human rights law.

17. However, many jurisdictions have not put such essential legal guardrails in place and do not have clear, precise, publicly available laws that govern hacking operations. […]

18. […] While, in certain circumstances, intrusive surveillance measures may be permissible under articles 17 and 19 of the International Covenant on Civil and Political Rights on grounds of the protection of national security or public order, hacking can never be justified for political or business reasons, which is often the case when human rights defenders or journalists are targeted.

19. Even if legitimate goals are being pursued, such as national security objectives or the protection of the rights of others, the assessment of the necessity and proportionality of the use of spyware severely limits the scenarios in which spyware would be permissible. […] Given the substantial adverse impacts of the use of spyware and its reach far beyond any intended target,

its use should be limited to cases where it would serve to prevent or investigate a specific serious crime or act amounting to a grave threat to national security. Its use should be narrowly targeted to an investigation of the person or persons suspected of committing or having committed such acts. This should be a last resort, in other words, all less intrusive measures should have been exhausted or have been shown to be futile, and should be strictly limited in scope and duration. Only relevant data should be accessed and collected. The measures should also be subject to rigorous independent oversight; prior approval by a judicial body is essential. In addition, robust and transparent export controls that explicitly take into account human rights risks can be a powerful tool for preventing rights violations and abuses. OHCHR reiterates its recent call as well as those of human rights experts and groups for a moratorium on the sale, transfer and use of hacking tools until a human rights-based safeguards regime is in place.

56. […] OHCHR recommends that States: (a) Ensure that any interference with the right to privacy, including hacking, restrictions to access and use of encryption technology and surveillance of the public, complies with international human rights law, including the principles of legality, legitimate aim, necessity and proportionality and non-discrimination, and does not impair the essence of that right;

57. […] OHCHR recommends that States: (a) Ensure that the hacking of personal devices is employed by authorities only as a last resort, used only to prevent or investigate a specific act amounting to a serious threat to national security or a specific serious crime, and narrowly targeted at the person suspected of committing those acts; such measures should be subject to strict independent oversight and should require prior approval by a judicial body;

Report of the United Nations High Commissioner for Human Rights, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests, UN Doc A/HRC/44/24 (24 June 2020)

26. […] The General Assembly has also recognized that States should refrain from employing unlawful or arbitrary surveillance techniques, which could include forms of hacking.

27. Despite these warnings, States continue to unduly resort to intrusive online surveillance and the hacking of the ICT tools used by those planning or organizing protests as well as protesters themselves. Surveillance software is used to infiltrate protesters smartphones, often after they are duped into downloading certain applications. These applications give unimpeded access to protesters' phones and their contacts, chat messages, phone conversations, and photos and videos shared on social media and communication platforms. Another cause for concern is the hacking of the social media accounts of protesters and organizers. Some State authorities use hacked devices to create false accounts to impersonate protest organizers and spread false information, or endanger followers, including through doxing (i.e., maliciously publishing personal information to encourage physical harm to protesters and organizers).

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

19. Governments appear to rely increasingly on offensive intrusion software that infiltrates individuals' digital devices. This type of hacking enables indiscriminate interception and collection of all kinds of communications and data, encrypted or not, and also permits remote and secret access to personal devices and data stored on them, enabling the conduct of real-time surveillance and manipulation of data on such devices. That poses risks not only for the right to privacy but also for procedural fairness rights when such evidence may be used in legal proceedings (see A/HRC/23/40, para. 62). […] Furthermore, hacking relies on exploiting vulnerabilities in information and communications technology (ICT) systems and thus contributes to security threats for millions of users. […]

38. Where Governments consider targeted hacking measures, they should take an extremely cautious approach, resorting to such measures only in exceptional circumstances for the investigation or prevention of the most serious crimes or threats and with the involvement of the judiciary (see CCPR/C/ITA/CO/6, para. 37). Hacking operations should be narrowly designed, limiting access to information to specific targets and types of information. States should refrain from compelling private entities to assist in hacking operations, thereby impacting the security of their own products and services. Compelled decryption may only be permissible on a targeted, case-by-case basis and subject to judicial warrant and the protection of due process rights (see A/HRC/29/32, para. 60).

Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, UN Doc CCPR/C/ITA/CO/6 (28 March 2017)

36. The Committee is concerned about reports alleging a practice of intercepting personal communications by intelligence agencies and the employment of hacking techniques by them without explicit statutory authorization or clearly defined safeguards from abuse. [...]

37. The State party should review the regime regulating the interception of personal communications, hacking of digital devices and the retention of communications data with a view to ensuring (a) that such activities conform with its obligations under article 17 including with the principles of legality, proportionality and necessity, (b) that robust independent oversight systems over surveillance, interception and hacking, including by providing for judicial involvement in the authorization of such measures in all cases and affording persons affected with effective remedies in cases of abuse, including, where possible, an ex post notification that they were subject to measures of surveillance or hacking

UN General Assembly Resolution on the Promotion and Protection of Human Right in the Context of Digital Technologies, UN Doc A/RES/78/213 (19 December 2023)

Noting with deep concern the use of technological tools developed by the private surveillance industry and by private or public actors to undertake surveillance, hacking of devices and systems, interception and disruption of communications, and data collection, interfering with the professional and private lives of individuals, including those engaged in the promotion and defence of human rights and fundamental freedoms, journalists and other media workers, in violation or abuse of their human rights,

UN Human Rights Council Resolution on the Promotion and protection of human rights in the context of peaceful protests, UN Doc A/HRC/RES/50/21 (8 July 2022)

31. *Expresses grave concern* at the use of private surveillance technologies to commit widespread violations and abuses against those exercising their right to peaceful assembly, including through hacking;

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN Doc A/78/520 (10 October 2023)

33. The ubiquity of sophisticated communications surveillance poses obvious threats to civil society actors' and organizations' rights to privacy and free expression, as well as such related rights as the freedom of assembly and association and the freedom to manifest one's religion. Many global study respondents reported experiences of digital surveillance and the transfer of their private data […], leading to deep concerns among civil society about permissive surveillance and data-sharing arrangements, and a dearth of regulation and due diligence with respect to both States and private

companies. The lack of regulation for private cybersecurity firms is profoundly concerning. The pernicious effect of unchecked and unregulated surveillance on civil society has been vividly demonstrated in the field of spyware. The position paper of the Special Rapporteur on the global regulation of the counter-terrorism spyware technology trade sets out in detail the inadequacy of the existing regulatory regime and identifies the minimum features of a rights-respecting approach to the unique challenge of spyware.

Report of the Special Rapporteur on the Independence of Judges and Lawyers, 'Reimagining justice: confronting contemporary challenges to the independence of judges and lawyers', UN Doc A/HRC/53/31 (13 April 2023)

66. Intrusive measures by States and businesses enable surveillance that feeds analysis, prediction and even manipulation of behaviour, at times to the detriment of free and fair elections and democratic processes. Recent revelations about global abuses of spyware, targeting journalists, human rights defenders, dissidents, opposition politicians and diplomats, are in flagrant violation of the right to privacy and the protection of personal data. […]

Report of the Special Rapporteur on the Promotion and Protection of Human Rights while Counter-Terrorism, Human Rights Implications of the Development, Use, Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism, UN Doc A/HRC/52/39 (1 March 2023)

44. Sophisticated surveillance technology developed for counter-terrorism and national security purposes has increasingly become a focus of international concern thanks to a spate of revelations demonstrating that such tools are in fact being used to spy on politicians, journalists, human rights activists, lawyers and ordinary citizens with no links to terrorism and who pose no national security threat. Intrusive covert technology for surveillance of the content of individuals' digital communications and other information, including metadata (location, duration, source and contacts) – commonly known as spyware – has proliferated internationally out of all control and poses substantial risks to the promotion and protection of human rights. […]

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association – Ten Years Protecting Civic Space Worldwide, UN Doc A/HRC/44/50 (13 May 2020)

68. Technological advances such as facial recognition, artificial intelligence, hacking tools and digital identification, are posing complex challenges to association and assembly rights. Governments are increasingly cutting off access to the Internet and mobile networks to stifle mass demonstrations and silent dissident voices during elections. For many in civil society, the Internet is no longer a safe place, as they have become the growing targets of surveillance and online violence. The slow progress in addressing these challenges points to the urgent need to move beyond commitments to action and accountability.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

25. [The Human Rights Committee] determined that the right to privacy required that robust, independent oversight systems were in place regarding surveillance, interception and hacking, including by ensuring that the judiciary was involved in the authorization of such measures, in all cases, and by affording persons affected with effective remedies in cases of abuse, including, where possible, an ex post notification that they had been placed under surveillance or that their data had been hacked (ibid., para. 37).

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, UN Doc A/HRC/41/41 (17 May 2019)

43. Some States have harnessed technology to monitor and hamper the work of human rights defenders and civil society actors. Tactics are varied. Many involve hacking phones and computers, issuing death and rape threats, disseminating doctored images, temporarily suspended targets' accounts, hijacking hashtags, spreading conspiracy theories, accusations of treason and promoting virulently discriminatory sentiments. While the Special Rapporteur is mindful that States are not the only perpetrators of these acts, government responsibility for these acts extends into the commissioning and encouragement of such conduct by third parties.

46. The use of commercial spyware, such as FinFisher monitoring technology and the Pegasus spyware suite, to launch cyberattacks against civil society actors is another example of this trend. Well-documented reports have linked the Pegasus spyware suite to spyware attacks against activists and human rights defenders in Bahrain, Kazakhstan, Mexico, Morocco, Saudi Arabia and the United Arab Emirates, among others. These attacks allow hacking into, and watching in real time, their communications, location and activities, and can affect targets both within a State or extraterritorially.

48. Women and lesbian, gay, bisexual, transgender and intersex persons are at particular risk of facing these attacks. […] These attacks take particular forms, which include the dissemination of doctored pictures, usually of a sexualized and gendered nature; the spreading of information designed to discredit, often full of harmful and negative gender stereotypes; violent hate messages and threatening messages on social networks, including calls for gang rape and for murder; and breaches of privacy, including hacking into family members' computers and phones and exposing the phone number, the home address and personal and family photos. […].

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/31/64 (8 March 2016)

39. The [Special Rapporteur on the Right to Privacy] firmly encourages the three committees of the UK Parliament commended above to continue, with renewed vigour and determination, to exert their influence in order that disproportionate, privacy-intrusive measures such as bulk surveillance and bulk hacking as contemplated in the Investigatory Powers Bill be outlawed rather than legitimised. It would appear that the serious and possibly unintended consequences of legitimising bulk interception and bulk hacking are not being fully appreciated by the UK Government... SRP invites the UK Government to show greater commitment to protecting the fundamental right to privacy of its own citizens and those of others and also to desist from setting a bad example to other states by continuing to propose measures, especially bulk interception and bulk hacking, which prima facie fail the standards of several UK Parliamentary Committees, run counter to the most recent Judgments of the European Court of Justice and the European Court of Human Rights, and undermine the spirit of the very right to privacy. […]

51. While some governments continue with ill-conceived, ill-advised, ill-judged, ill-timed and occasionally ill-mannered attempts to legitimise or otherwise hang on to disproportionate, unjustifiable privacy-intrusive measures such as bulk collection, bulk hacking, warrantless interception etc. other governments led, in this case by the Netherlands and the USA have moved more openly towards a policy of no back doors to encryption. The SRP would encourage many more governments to coalesce around this position.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/23/40 (17 April 2013)

62. […] Offensive intrusion software such as Trojans, or mass interception capabilities, constitute such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information. There are not just new methods for conducting surveillance; they are new forms of surveillance. From a human rights perspective, the use of such technologies is extremely disturbing. Trojans, for example, not only enable a State to

access devices, but also enable them to alter – inadvertently or purposefully – the information contained therein. This threatens not only the right to privacy but also procedural fairness rights with respect to the use of such evidence in legal proceedings.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/20/17 (4 June 2012)

63. Additionally, the Special Rapporteur is deeply concerned by harassment of online journalists and bloggers, such as illegal hacking into their accounts, monitoring of their online activities... and the blocking of websites that contain information that are critical of authorities. Such actions constitute intimidation and censorship.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/17/27 (16 May 2011)

51. Cyber-attacks, or attempts to undermine or compromise the function of a computer-based system, include measures such as hacking into accounts or computer networks, and often take the form of distributed denial of service (DDoS) attacks... such attacks are sometimes undertaken during key political moments. The Special Rapporteur also notes that websites of human rights organizations and dissidents are frequently and increasingly becoming targets of DDoS attacks [...]

52. When a cyber-attack can be attributed to the State, it clearly constitutes inter alia a violation of its obligation to respect the right to freedom of opinion and expression. Although determining the origin of cyber-attacks and the identity of the perpetrator is often technically difficult, it should be noted that States have an obligation to protect individuals against interferences by third parties that undermines the enjoyment of the right to freedom of opinion and expression. This positive obligation to protect entails that States must take appropriate and effective measures to investigate actions taken by third parties, hold the persons responsible to account, and adopt measures to prevent such recurrence in the future.

Concluding Observations on the Fifth Periodic Report of the Netherlands, Human Rights Committee, UN Doc CCPR/C/NLD/CO/5 (22 August 2019)

54. The Committee is concerned about the Intelligence and Security Services Act 2017, which provides the intelligence and security services with sweeping surveillance and interception powers, including bulk data collection. It is particularly concerned that the Act does not provide for a clear definition of case-specific bulk data collection; clear grounds for extending retention periods for information collected; and adequate safeguards against bulk data hacking. It is also concerned by the limited practical possibilities for complaining, in the absence of a comprehensive notification regime, to the Review Committee on the Intelligence and Security Services (art. 17).

55. The State party should review the Act with a view to bringing its definitions and the powers and limits on their exercise in line with the Covenant and strengthen the independence and effectiveness of the two new bodies established by the Act, the Evaluation Committee on the Use of Powers and the Review Committee on the Intelligence and Security Services.

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Concern Over the Acquisition and Implementation of Surveillance Programs by States of the Hemisphere, Press Release R80/15 (21 July 2015)

In recent days, at least 400 GB of information were publicly exposed from the Italian firm *Hacking Team*, a company dedicated to the commercialization of the Remote Control System (RCS) spying software provided to government and government agencies. […] The surveillance software commercialized by the company is designed to evade computers or mobile phones' encryption, allowing the gathering of information, messages, calls and emails, voice over IP and chat

communication from everyday devices. This software can also remotely activate microphones and cameras. […] On this disclosure, and facing possible impacts derived from the usage of this type of privacy-invading technologies and the right to exercise freedom of expression without illegal interferences, the Office of the Special Rapporteur would like to recall that according to international standards, the use of programs or systems for the surveillance of private communications should be clearly and precisely established by law, genuinely exceptional and selective, and must be strictly limited to the needs to meet compelling objectives such as the investigation of serious crime as defined in legislation. Such restrictions must be strictly proportionate and consistent with the international standards of the right to freedom of expression. This Office has stated that the surveillance of communications and the interference in privacy that exceeds what is stipulated by law, which are oriented to aims that differ from those which the law permits or are carried out clandestinely, must be harshly punished. Such illegitimate interference includes actions taken for political reasons against journalists and independent media.

C. BIOMETRIC DATA PROCESSING IN SURVEILLANCE

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

Recognizing that, while the use of artificial intelligence can have significant positive economic and social impacts, it requires and allows for the processing of large amounts of data, often relating to personal data, including biometric data and data on an individual's behaviour, social relationships, race or ethnicity, religion or belief, which can pose serious risks to the enjoyment of the right to privacy, especially when done without proper safeguards, in particular when employed for identification, tracking, profiling, facial recognition, classification, behaviour prediction or scoring of individuals,

Emphasizing that unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data, hacking and the unlawful use of biometric technologies, as highly intrusive acts, violate the right to privacy, […] including when undertaken extraterritorially or on a mass scale,

Noting the increase in the collection of sensitive biometric information from individuals, and stressing that States must comply with their human rights obligations and that business enterprises should respect the right to privacy and other human rights when collecting, processing, sharing and storing biometric information by, inter alia, considering the adoption of data protection policies and safeguards,

6. *Acknowledges* that the conception, design, use, deployment and further development of new and emerging technologies, such as those that involve artificial intelligence, may have an impact on the enjoyment of the right to privacy and other human rights, and that the risks to these rights can and should be avoided and minimized by adapting or adopting adequate regulation or other appropriate mechanisms, […]"

** See also UN* General *Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014)*

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

Recognizing that, despite its positive effects, the use of digital technologies and artificial intelligence systems that require the processing of large amounts of data, often relating to personal data, including on an individual's behaviour, social relationships, private preferences and identity, including metadata, can pose serious risks to the right to privacy, in particular when employed for identification, tracking, profiling, facial recognition, behavioural prediction or the scoring of individuals,

Noting that the use of data extraction and algorithms to target content towards online users may undermine user agency and access to information online, as well as the right to freedom of opinion and expression,

Noting with concern the intrusiveness and impact of data-gathering practices, the related impacts and harms stemming from surveillance and the increasing use of algorithms involved in the application of artificial intelligence systems,

Noting with concern also that certain predictive algorithms and the increasing use of facial recognition and surveillance technologies are likely to result in discrimination, in particular when data used in the training of algorithms are not accurate, relevant and representative and audited against encoded bias,

Noting that the use of artificial intelligence may, without human rights safeguards, pose the risk of reinforcing discrimination, including structural inequalities, especially when processing sensitive data, and recognizing that racially and otherwise discriminatory outcomes must be prevented in the design, development, implementation and use of new and emerging digital technologies,

Noting with concern reports indicating lower accuracy of biometric data identification, including facial recognition technologies that show racial identification biases and prejudices against women, including when non-representative training data are used, and that the use of digital technologies can reproduce, reinforce and even exacerbate racial and gender inequalities, and recognizing in this context the importance of effective remedies,

Acknowledging that, while metadata may provide benefits, certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications and can give an insight into an individual's behaviour, including their movements, social relationships, political activities, private preferences and identity, and as such recalling that service providers should take steps to minimize, obscure or delete metadata and to reduce the traceability of users' metadata in order to strengthen the protections afforded by encryption and protect the right to privacy,

2. *Also recalls* the increasing impact of new and emerging technologies, such as those developed in the fields of surveillance, artificial intelligence, automated decision-making and machine-learning, and of profiling, tracking and biometrics, including facial recognition, without human rights safeguards, present to the full enjoyment of the right to privacy and other human rights, and acknowledges that some applications may not be compatible with international human rights law;

7. *Also stresses* that remote biometric surveillance systems, including facial recognition, raise serious concerns with regard to their proportionality, given their highly intrusive nature and broad impact on large numbers of people;

10. Calls upon all States:

(c) To review, on a regular basis, their procedures, practices and legislation regarding the surveillance of communications, including mass surveillance and the interception and collection of personal data, as well as regarding the use of profiling, automated decision-making, machine learning and biometric technologies, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(f) To ensure that biometric identification and recognition technologies, including facial recognition technologies by public and private actors, do not enable arbitrary or unlawful surveillance, including of those exercising their right to freedom of peaceful assembly;

(g) To ensure that digital or biometric identity programmes are designed, implemented and operated after appropriate technical, regulatory, legal and ethical safeguards are in place and in

full compliance with the obligations of States under international human rights law;

** See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019);*

UN Human Rights Council Resolution on New and Emerging Digital Technologies and Human Rights, UN Doc A/HRC/RES/53/29 (14 July 2023)

Recognizing further that artificial intelligence systems, when used without appropriate safeguards and including when used for identification, tracking, profiling, facial recognition, the generation of synthetic photorealistic images, behavioural prediction or the scoring of individuals, can entail serious risks for the protection, promotion and enjoyment of human rights, such as, inter alia, the rights to privacy, to freedom of opinion and expression, to freedom of thought, conscience and religion, the rights to equal protection of the law and to a fair and public hearing, as well as economic, social and cultural rights, in particular by embedding and exacerbating bias, which potentially results in discrimination and inequality, and by intensifying threats from misinformation, disinformation and hate speech, which may lead to violence, including political violence, and stressing that certain applications of artificial intelligence present an unacceptable risk to human rights, […]

3. *Highlights* the importance of the need to respect, protect and promote human rights and fundamental freedoms, in recognition of the inherent dignity of the human person, throughout the lifecycle of artificial intelligence systems and, towards this end, the need to pay particular attention to: (e) Strengthening, as necessary, the oversight and enforcement capacity of respective States relevant to artificial intelligence and sectors where artificial intelligence is being applied to allow more effective measures to protect against human rights risks relating to artificial intelligence; (f) Promoting research and the sharing of best practices on ensuring transparency, human oversight and accountability in relation to the uses of artificial intelligence systems in ways that prevent and avoid the spread of disinformation and hate speech […].

Report of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/48/31 (13 September 2021)

23. AI systems are often used as forecasting tools. They use algorithms to analyse large quantities of data, including historic data, to assess risks and predict future trends. Depending on the purpose, training data and data analysed can include, for example, criminal records, arrest records, crime statistics, records of police interventions in specific neighbourhoods, social media posts, communications data and travel records. The technologies may be used to create profiles of people, identify places as likely to be sites of increased criminal or terrorist activity, and even flag individuals as likely suspects and future reoffenders.

25. Developments in the field of biometric recognition technology have led to its increasing use by law enforcement and national security agencies. Biometric recognition relies on the comparison of the digital representation of certain features of an individual, such as the face, fingerprint, iris, voice or gait, with other such representations in a database. From the comparison, a higher or lower probability is deduced that the person is indeed the person to be identified. These processes are increasingly carried out in real time and from a distance. In particular, remote real-time facial recognition is increasingly deployed by authorities across the globe.

26. Remote real-time biometric recognition raises serious concerns under international human rights law, which the High Commissioner has highlighted previously. Some of these concerns reflect the problems associated with predictive tools, including the possibility of erroneous identification of individuals and disproportionate impacts on members of certain groups. Moreover,

facial recognition technology can be used to profile individuals on the basis of their ethnicity, race, national origin, gender and other characteristics.

27. Remote biometric recognition is linked to deep interference with the right to privacy. A person's biometric information constitutes one of the key attributes of her or his personality as it reveals unique characteristics distinguishing her or him from other persons. Moreover, remote biometric recognition dramatically increases the ability of State authorities to systematically identity and track individuals in public spaces, undermining the ability of people to go about their lives unobserved and resulting in a direct negative effect on the exercise of the rights to freedom of expression, of peaceful assembly and of association, as well as freedom of movement. Against this background, the High Commissioner therefore welcomes recent efforts to limit or ban the use of real-time biometric recognition technologies.

59. The High Commissioner recommends that States: […] (b) Ensure that the use of AI is in compliance with all human rights and that any interference with the right to privacy and other human rights through the use of AI is provided for by law, pursues a legitimate aim, complies with the principles of necessity and proportionality and does not impair the essence of the rights in question; […] (d) Impose a moratorium on the use of remote biometric recognition technologies in public spaces, at least until the authorities responsible can demonstrate compliance with privacy and data protection standards and the absence of significant accuracy issues and discriminatory impacts, and until all the recommendations set out in A/HRC/44/24, paragraph 53 (j) (i–v), are implemented; […]

UN General Assembly Resolution on the Promotion and Protection of Human Right in the Context of Digital Technologies, UN Doc A/RES/78/213 (19 December 2023)

20. *Calls upon* Member States and, where applicable, other stakeholders: (d) To ensure that digital or biometric identity programmes are designed, implemented and operated after appropriate human rights standards, as well as technical, regulatory, legal and ethical safeguards, are in place, and in line with international human rights law;

UN Human Rights Council Resolution on the Promotion and protection of human rights in the context of peaceful protests, UN Doc A/HRC/RES/50/21 (8 July 2022)

29. *Urges* States to refrain from the arbitrary or unlawful use of biometric identification technologies, including facial recognition, to identify those peacefully participating in an assembly;

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019)

Noting the increase in the collection of sensitive biometric information from individuals, and stressing that States must respect their human rights obligations and that business enterprises should respect the right to privacy and other human rights when collecting, processing, sharing and storing biometric information by, inter alia, adopting of data protection policies and safeguards,

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

57. […] OHCHR recommends that States: (d) […] biometric recognition systems should only be used in public spaces to prevent or investigate serious crimes or serious public safety threats and if all requirements under international human rights law are implemented with regard to public spaces;

Report of the United Nations High Commissioner for Human Rights, Impact of New

Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests, UN Doc A/HRC/44/24 (24 June 2020)

24. Safe and confidential communications play a key role in the planning and holding of peaceful protests. Technology-enabled surveillance poses significant risks to the enjoyment of human rights in peaceful assemblies and is an important contributor to the shrinking of civic space in many countries. New technologies have significantly expanded the abilities of State authorities to surveil protests, protest organizers and participants. These technologies are used to monitor the planning and organization of protests – for example, through the hacking of the digital tools used by those seeking to assemble. They are also used to conduct surveillance during protests – for example, through the use of biometrics-based facial recognition technology and the interception of communications. In response to this trend, the Human Rights Council has underlined the importance of privacy online for the realization of the rights of peaceful assembly and association. […]

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN Doc A/78/520 (10 October 2023)

35. The Special Rapporteur further addresses how biometrics surveillance systems have been controversially used and underscores the threats to the life, security and privacy of civil society actors from the misuse of biometric data collection processes.

Report of the Working Group on Enforced and Involuntary Disappearances, 'New technologies and enforced disappearances', UN Doc A/HRC/54/22/Add.5 (11 September 2023)

23. According to the information received by the Working Group, the above-mentioned surveillance technologies, as well as artificial intelligence solutions, drones, thermal imaging sensors, night-vision googles, biometric identification systems, aerial surveillance towers and specialised sensors for detecting mobile phone emissions and tracking devices, have increasingly been used at borders by States and regional agencies to automate processes of identifying and tracking the movement of migrants, refugees and asylum seekers, including in pushback operations, leading – or in some instances amounting – to enforced disappearances. The Working Group learned also about the failure to use data gathered through the said technologies with Search and Rescue teams and authorities, thus failing to prevent migrants in distress from going missing or dying. The Working Group expresses deep concern vis-à-vis such a vicious use of new technologies and notes that the applicable international legal framework – especially concerning the use of artificial intelligence – is flawed and should be urgently strengthened.

65. […] the Working Group recommends that States:

(k) Guarantee that collection, retention and use of biometric and genetic data is regulated in law and in practice, is narrow in scope, transparent, necessary and proportionate to meeting a legitimate security goal, and is not based on any distinction, exclusion, restriction or preference based on race, colour, descent or national or ethnic origin;

(l) Review, through a multi-disciplinary process, the adequacy of the applicable policies and legal frameworks, to devise strategies to prevent and address negative impact on human rights generated by the use of new technologies, including machine-learning and artificial intelligence;

(m) Ensure that mass and targeted surveillance technologies, as well as AI and machine-learning solutions, are not used at borders for the purposes of performing pushback operations that may lead, and in certain cases amount to, enforced disappearance. Data on migratory movements gathered through these technologies should be used for facilitating search and rescue operations and for humanitarian purposes;

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and

Association, 'Protection of human rights in the context of peaceful protests during crisis situations', UN Doc A/HRC/50/42 (16 May 2022)

78. In regard to respecting and enabling peaceful protest during crisis situations, States should: (m) Refrain from the use of biometric identification and recognition technologies, such as facial recognition, for arbitrary surveillance of protesters, both offline and online;

Report of the Special Rapporteur on the Promotion and Protection of Human Rights while Counter-Terrorism, Human Rights Implications of the Development, Use, Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism, UN Doc A/HRC/52/39 (1 March 2023)

20. The Special Rapporteur, among others, has raised concerns regarding the collection of the biometric data of vulnerable populations and persons in diverse contexts. The collection of biometric data of populations in conflict zones, including in Iraq and Afghanistan, has raised serious concerns, including with respect to the transfer of biometric data collected under the rubric of countering terrorism directly into the hands of United Nations-designated terrorist groups or individuals. Special procedure mandate holders and the Committee on the Elimination of Racial Discrimination have raised concerns about the use of such technologies in the Xinjiang Uyghur Autonomous Region in the context of the application by China of its Counter-Terrorism Law and its implementing measures in the region. Among a slate of measures raising serious human rights concerns, reports indicate that authorities have conducted mass collection of biometric data (such as DNA samples, fingerprints, iris scans and blood types) of residents of the region. The use of biometric data in Somalia and by Israel in the Occupied Palestinian Territory has raised similar concerns.

21. She highlights that the coronavirus disease (COVID-19) pandemic has accelerated biometric data collection and both further exceptionalized and normalized its use, including the deployment of biometric capacity developed for counter-terrorism and security purposes to the management of a global health pandemic that has disproportionately affected religious, ethnic and racial minorities, other vulnerable groups and those economically and socially marginalized in society. The repurposing of biometric capacity developed for counter-terrorism purposes to regulate the most marginal communities during a pandemic should concern all stakeholders.

23. This concerted policy drive towards comprehensive biometrics collection has not been undergirded by the necessary work to achieve an adequate worldwide legal and regulatory regime. Indeed, instead of leading a comprehensive effort to agree on a set of robust international rules and standards regarding biometric/identity data collection, the chief effort in the United Nations system has simply been a capacity-building programme to facilitate that collection. […]

24. The Special Rapporteur's particular concerns regarding the Programme and the system of personal data collection it supports include: (a) the collection of data in principle, given the degree of detail that the data, particularly passenger name record data, provide about the data subjects' lives; (b) the way in which the collection, by definition and unavoidably, occurs in relation to all travelers without discrimination, raising a clear challenge to necessity and proportionality; (c) the length of the retention period, which takes the use of such data beyond being merely a check against watchlists for particular flights and renders it capable of being a long-term record of personal behaviour from which detailed knowledge can be drawn; and (d) the data-sharing across borders between agencies of different nations raises particular risks with respect to differing standards of human rights compliance internationally. The Special Rapporteur is deeply concerned about inaccurate/discriminatory algorithmic decision-making in advance passenger information and passenger name records; she underscores the impact of the use or transfer of these technologies on freedom of movement, the right to leave and the right to seek asylum; and she highlights illegitimate targeting by States to whom data are transferred and the entirely inadequate remedies that exist for breaches of human rights that occur in the context of the use of such data. She notes the limited engagement of the Programme with United Nations human rights entities. She calls for

an independent audit of the Programme to ensure the integrity of its practices and technology transfer in respect of human rights, data protection and the rule of law.

26. She also highlights her profound concerns about biometric data-sharing, which is strongly encouraged by the international community. One striking motif of normative counter-terrorism regulation has been the increased emphasis on the cooperation between States to advance presumed convergent counter-terrorism interests. Data-sharing is a black box of international law practice, with little information available on whether and what type of biometric data are exchanged, and, more practically, on the content of data-sharing agreements. Whether human rights considerations figure at all in such agreements remains largely unknown. She highlights the tension that currently exists between repeated calls by the General Assembly and the Human Rights Council for counter-terrorism cooperation among States, in instruments from the Global Counter-Terrorism Strategy to resolutions, and the abject failure to specify that such cooperation must be undertaken in compliance with States' human rights obligations, including with regard to the right to privacy.

Report of the Special Rapporteur on the Right to Privacy: Artificial Intelligence and Privacy, and Children's Privacy, UN Doc A/HRC/46/37 (25 January 2021)

95. Biometric surveillance and tracking technologies used to identify and monitor children suspected of wrongdoing was reported from South America, as was the failure to protect children's privacy during judicial processes. Identifying children of interest to law enforcement authorities or the offspring of incarcerated parents or of parents associated with terrorism contravenes privacy, leading to stigmatization and discrimination and impairing the development of personality. Development can be constrained also when those children are not identified to relevant support services, although data sharing can be problematic, particularly with security personnel.

127. The Special Rapporteur recommends that States:

(m) Prior to the linking of civil and criminal identity databases, undertake human rights impact assessments on the implications for children and their privacy, and conduct consultations to assess the necessity, proportionality and legality of biometric surveillance;

(p) Ensure that biometric data is not collected from children, unless as an exceptional measure only when lawful, necessary, proportionate and fully in line with the rights of the child;

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/43/52 (24 March 2020)

48. States and non-State actors should: (e) Ensure that: (v) The processing of biometric data is undertaken only if there are no other less intrusive means available and only if accompanied by appropriate safeguards, including scientifically recognized methods, and strict security and proportionality protocols;

Concluding Observations on the Eighth Periodic Report of the Russian Federation, Human Rights Committee, UN Doc CCPR/C/RUS/CO/8 (1 November 2022)

32. […] It is concerned about reports that participation in assemblies is hampered by the use of preventive detention and by the use of facial recognition systems that are not regulated by law, including in regard to the procedure for storing and reviewing data relating to such systems (arts. 7, 9–10, 14, 17, 19 and 21).

33. In accordance with article 21 of the Covenant and in the light of the Committee's general comment No. 37 (2020) on the right of peaceful assembly, the State party should: (e) Refrain from the use of facial recognition systems and the practice of preventive detention to hamper participation in peaceful assemblies.

Concluding Observations on the Third Periodic Report of Lebanon, Human Rights Committee, UN Doc CCPR/C/LBN/CO/3 (9 May 2018)

33. The Committee is concerned about reports of arbitrary interference with the privacy of individuals, including […] allegations of direct authorizations by the Prime Minister of the interception of private communications and access to data without the prior judicial authorization required by law; and the granting of full telecommunications data access to security agencies, following the relinquishment of the authority of the Council of Ministers to approve or deny such requests. The Committee is also concerned about the insufficient protection of biometric data under the current legal framework and notes that a bill on this issue was submitted to the Standing Committee of the Parliament (arts. 2 and 17).

34. The State party should ensure that all laws governing surveillance activities, access to personal data and communications data (metadata) and any other interference with privacy are in full conformity with the Covenant, in particular article 17, including as regards the principles of legality, proportionality and necessity, and that State practice conforms thereto. It should, inter alia, ensure that (a) surveillance, collection of, access to and use of data and communications data are tailored to specific legitimate aims, are limited to a specific number of persons and are subject to judicial authorization; (b) effective and independent oversight mechanisms are in place to prevent arbitrary interference with privacy; and […] The State party should also ensure biometric data protection guarantees, in accordance with article 17 of the Covenant.

Concluding Observations on the Third Periodic Report of Kuwait, Human Rights Committee, UN Doc CCPR/C/KWT/CO/3 (11 August 2016)

20. The Committee is concerned that Law No. 78 (2015) on counter-terrorism, which requires nationwide compulsory DNA testing and the creation of a database under the control of the Minister of the Interior, imposes unnecessary and disproportionate restrictions on the right to privacy. The Committee is particularly concerned about: (a) The compulsory nature and the sweeping scope of DNA testing, which applies to all and imposes a penalty of one year's imprisonment and a fine in case of refusal to provide samples; (b) The broad powers of the authorities and the Ministry of the Interior to collect and use DNA samples, including "for any other cases required by the supreme interest of the country"; (c) The lack of clarity on whether necessary safeguards are in place to guarantee the confidentiality and prevent the arbitrary use of the DNA samples collected; (d) The absence of independent control and the inability to challenge the law before an independent court.

21. The State party should take all measures necessary to ensure that DNA samples are collected, used and retained in conformity with its obligations under the Covenant, including article 17, and that any interference with the right to privacy complies with the principles of legality, necessity and proportionality. Specifically, the State party should: (a) amend Law No. 78 (2015) with a view to limiting DNA collection to individuals suspected of having committed serious crimes and on the basis of a court decision; (b) ensure that individuals can challenge in court the lawfulness of a request for the collection of DNA samples; (c) set a time limit after which DNA samples are removed from the database; and (d) establish an oversight mechanism to monitor the collection and use of DNA samples, prevent abuses and ensure that individuals have access to effective remedies.

***Glukhin v Russia*, App No 11519/20, Judgment, European Court of Human Rights (04 July 2023)**

65. The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding. However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the

records, the way in which these records are used and processed and the results that may be obtained (see and *Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 67, ECHR 2008).

66. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor in this assessment. As to the monitoring of an individual's actions using photographic or video devices, the Convention institutions have taken the view that the monitoring of the actions and movements of an individual in a public place using a camera which did not record the visual data does not constitute in itself a form of interference with private life. Private-life considerations may arise, however, once any systematic or permanent record of such personal data comes into existence, particularly pictures of an identified person. A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right of each person to the protection of his or her image is thus one of the essential components of personal development and presupposes the right to control the use of that image. While in most cases the right to control such use involves the possibility for an individual to refuse publication of his or her image, it also covers the individual's right to object to the recording, conservation and reproduction of the image by another person (see *López Ribalda and Others*, cited above, 89, with further references).

67. The Court has previously found that the collection and storing of data by the authorities on particular individuals constituted an interference with those persons' private lives, even if that data concerned exclusively the person's public activities (see *Amann v. Switzerland* [GC], no. 27798/95, §§ 65-67, ECHR 2000-II, and *Rotaru v. Romania* [GC], no. 28341/95, §§ 43-44, ECHR 2000-V), such as participation in anti-government demonstrations (see *Association "21 December 1989" and Others v. Romania*, nos. 33810/07 and 18817/08, § 170, 24 May 2011, and *Catt v. the United Kingdom*, no. 43514/15, 93, 24 January 2019). It has also found that the following instances of collection of data in a public place constituted an interference with the persons' private lives: the recording of a questioning in a public area of a police station (see *P.G. and J.H. v. the United Kingdom*, no. 44787/98, §§56-60, ECHR 2001-IX); recording by CCTV cameras in a public place and the subsequent disclosure of the video-footage to the media (see *Peck v. the United Kingdom*, no. 44647/98, §§ 57-63, ECHR 2003-I); recording of video-footage at a police station and its subsequent use in criminal proceedings (see *Perry v. the United Kingdom*, no. 63737/00, §§ 36-43, ECHR 2003-IX (extracts); the collection, through a GPS device attached to a person's car, and storage of data concerning that person's whereabouts and movements in the public sphere (see *Uzun v. Germany*, no. 35623/05, §§ 51-53, ECHR 2010 (extracts), and *Ben Faiza v. France*, no. 31446/12, §§ 53-55, 8 February 2018); the registration of a person's name in a police database which automatically collected and processed information about that person's movements, by train or air (see *Shimovolos v. Russia*, no. 30194/09, § 66, 21 June 2011); and video surveillance of university amphitheatres at a public university (see *Antović and Mirković v. Montenegro*, no. 70838/13, §§ 40-45 and 55, 28 November 2017).

68. In the present case, during routine monitoring of the Internet the police discovered photographs and a video of the applicant holding a solo demonstration published on a public Telegram channel. They made screenshots of the Telegram channel, stored them and allegedly applied facial recognition technology to them to identify the applicant. Having identified the location on the video as one of the stations of the Moscow underground, the police also collected video-recordings from CCTV surveillance cameras installed at that station as well as at two other stations through which the applicant had transited. They made screenshots of those video-recordings and stored them. They also allegedly used the live facial recognition CCTV cameras installed in the Moscow underground to locate and arrest the applicant several days later with the aim of charging him with an administrative offence. The screenshots of the Telegram channel and of the video-recordings from the CCTV surveillance cameras were subsequently used in evidence in the administrative-offence proceedings against the applicant (see paragraphs 7-15 above).

70. As regards the applicant's identification from the photographs and the video published on Telegram, the Court notes that although the photographs and the video in question did not contain any information permitting the identification of the applicant, he was identified within less than two days. The police report (see paragraph 11 above) did not explain which operational-search measures had been taken to identify him. The applicant's attempt to challenge the lawfulness of such measures failed, as the courts summarily dismissed his complaints (see paragraphs 16-17 above). In such circumstances it was not unreasonable for the applicant to assume that facial recognition technology had been used in his case. The Government did not explicitly deny this or provide any clarifications as to the measures used to identify the applicant. Lastly, the Court takes note of public information available regarding numerous cases involving the use of facial recognition technology to identify participants of protest events in Russia (see paragraph 40 above).

72. Against this background, and taking into account the difficulty for the applicant to prove his allegations because the domestic law did not provide for an official record or notification of the use of facial recognition technology, the absence of any other explanation for the rapid identification of the applicant, and the implicit acknowledgment by the Government of the use of live facial recognition technology, the Court accepts in the particular circumstances of the case that facial recognition technology was used. The Court has previously found that the storage of photographs by the police, coupled with a possibility of applying facial recognition techniques to them, constituted an interference with the right to private life (see *Gaughran v. the United Kingdom*, no.45245/15, §§ 69-70, 13 February 2020).

73. The Court concludes that the processing of the applicant's personal data in the framework of the administrative offence proceedings against him, including the use of facial recognition technology – first, to identify him from the photographs and the video published on Telegram and, secondly, to locate and arrest him later while he was travelling on the Moscow underground – amounted to an interference with his right to respect for his private life within the meaning of Article 8 § 1 of the Convention.

75. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes (see *S. and Marper*, cited above, § 103), and especially where the technology available is continually becoming more sophisticated (see *Catt*, cited above, § 114; *Gaughran*, cited above, § 86; and *Uzun*, cited above, § 61). The protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests (see *S. and Marper*, cited above, § 112).

76. Personal data revealing political opinions, such as information about participation in peaceful protests, fall in the special categories of sensitive data attracting a heightened level of protection (see *Catt*, cited above, §§ 112 and 123).

77. In the context of the collection and processing of personal data, it is therefore essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness (see *S. and Marper*, cited above, § 99, and *P.N. v. Germany*, no. 74440/17, § 62, 11 June 2020).

82. In so far as the applicant alleged that the domestic law did not meet the "quality of law" requirement, the Court considers that it is essential in the context of implementing facial recognition technology to have detailed rules governing the scope and application of measures as well as strong safeguards against the risk of abuse and arbitrariness. The need for safeguards will be all the greater where the use of live facial recognition technology is concerned.

83. The Court has strong doubts that the domestic legal provisions meet the "quality of law" requirement. It notes, in particular, that the domestic law permits the processing of biometric personal data "in connection with the administration of justice" (see paragraph 31 above). This legal provision is widely formulated. Taking into account that the Government did not refer to any authoritative interpretation of that provision by the Supreme or Constitutional Courts or submit any examples of its restrictive interpretation and application in administrative and judicial practice, it appears that it allows processing of biometric personal data – including with the aid of facial recognition technology – in connection with any judicial proceedings. The domestic law does not contain any limitations on the nature of situations which may give rise to the use of facial recognition technology, the intended purposes, the categories of people who may be targeted, or on processing of sensitive personal data. Furthermore, the Government did not refer to any procedural safeguards accompanying the use of facial recognition technology in Russia, such as the authorisation procedures, the procedures to be followed for examining, using and storing the data obtained, supervisory control mechanisms and available remedies.

***P.N. v Germany*, App No 74440/17, Judgment, European Court of Human Rights (11 June 2020)**

56. […] The taking of a person's photograph and its retention in a police database with the possibility of it being processed automatically constitutes an interference with the right to respect for private life under Article 8 of the Convention […].

57. The taking and storage on the national authorities' records of the fingerprints of an identified or identifiable individual also amounts to an interference with that person's right to respect for private life […].

58. Likewise, the storing by a public authority of information relating to an individual's private life, such as contact details of convicted persons, is an interference with that right […].

59. In the present case, the police ordered that photographs as well as fingerprints and palm prints be taken from the applicant and a description of his person be drawn up for the police records; this was designed to serve future identification purposes. That order was subsequently executed […]. The Court, having regard to its case-law, considers that the taking and storage of these various types of personal data amount to interference with the applicant's right to respect for his private life.

60. […] as the Court has previously considered that even the storing of contact details of a convicted offender by a public authority was an interference with the individual's right to respect for private life, Article 8 is likewise applicable to the applicant's physical description and its inclusion in the police records.

***Gaughran v The United Kingdom*, App No 45245/15, Judgment, European Court of Human Rights (13 February 2020)**

66. […] in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained.

67. In that connection, the Court notes that the photograph of the applicant was taken on his arrest

to be stored indefinitely on the local police database. At the time of its judgment in 2014 the Supreme Court found that the applicant's custody photograph was held on a standalone database, limited to authorised police personnel and which did not have the capability to match photographs whether by way of facial recognition or otherwise […].

70. […] In the present case, given that the applicant's custody photograph was taken on his arrest and will be held indefinitely on a local database for use by the police and that the police may also apply facial recognition and facial mapping techniques to the photograph, the Court has no doubt that the taking and retention of the applicant's photograph amounts to an interference with his right to private life within the meaning of Article 8 § 1.

75. […] Accordingly, it considers that retention of biometric data and photographs pursues the legitimate purpose of the detection and, therefore, prevention of crime. While the original taking of this information pursues the aim of linking a particular person to the particular crime of which he or she is suspected, its retention pursues the broader purpose of assisting in the identification of persons who may offend in the future.

94. Having chosen to put in place a regime of indefinite retention, there was a need for the State to ensure that certain safeguards were present and effective for the applicant […], someone convicted of an offence […]. However, the applicant's biometric data and photographs were retained without reference to the seriousness of his offence and without regard to any continuing need to retain that data indefinitely. Moreover, the police are vested with the power to delete biometric data and photographs only in exceptional circumstances […]. There is no provision allowing the applicant to apply to have the data concerning him deleted if conserving the data no longer appeared necessary in view of the nature of the offence, the age of the person concerned, the length of time that has elapsed and the person's current personality […]. Accordingly, the review available to the individual would appear to be so narrow as to be almost hypothetical […].

96. […] that widened margin is not sufficient for it to conclude that the retention of such data could be proportionate in the circumstances, which include the lack of any relevant safeguards including the absence of any real review.

97. Accordingly, the respondent State has overstepped the acceptable margin of appreciation in this regard and the retention at issue constitutes a disproportionate interference with the applicant's right to respect for private life and cannot be regarded as necessary in a democratic society.

***S. and Marper v The United Kingdom*, Apps Nos 30562/04 and 30566/04, Judgment, European Court of Human Rights (4 December 2008)**

67. The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (see Leander v. Sweden, 26 March 1987, § 48, Series A no. 116). The subsequent use of the stored information has no bearing on that finding (see *Amann v. Switzerland* [GC], no. 27798/95, § 69, ECHR 2000-II). However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained (see, mutatis mutandis, *Friedl*, cited above, §§ 49-51, and Peck, cited above, § 59).

68. The Court notes at the outset that all three categories of the personal information retained by the authorities in the present case, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of the Data Protection Convention as they relate to identified or identifiable individuals. […]

69. […] As regards the nature and scope of the information contained in each of these three

categories of data, the Court has distinguished in the past between the retention of fingerprints and the retention of cellular samples and DNA profiles in view of the stronger potential for future use of the personal information contained in the latter (see *Van der Velden v. the Netherlands* (dec.), no. 29514/05, ECHR 2006-XV). The Court considers it appropriate to examine separately the question of interference with the applicants' right to respect for their private lives by the retention of their cellular samples and DNA profiles on the one hand, and of their fingerprints on the other.

(i) Cellular samples and DNA profiles

71. The Court maintains its view that an individual's concern about the possible future use of private information retained by the authorities is legitimate and relevant to a determination of the issue of whether there has been an interference. Indeed, bearing in mind the rapid pace of developments in the field of genetics and information technology, the Court cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today. Accordingly, the Court does not find any sufficient reason to depart from its finding in the *Van der Velden* case.

72. Legitimate concerns about the conceivable use of cellular material in the future are not, however, the only element to be taken into account in the determination of the present issue. In addition to the highly personal nature of cellular samples, the Court notes that they contain much sensitive information about an individual, including information about his or her health. Moreover, samples contain a unique genetic code of great relevance to both the individual and his relatives. […]

73. Given the nature and the amount of personal information contained in cellular samples, their retention per se must be regarded as interfering with the right to respect for the private lives of the individuals concerned. That only a limited part of this information is actually extracted or used by the authorities through DNA profiling and that no immediate detriment is caused in a particular case does not change this conclusion (see *Amann*, cited above, § 69).

74. As regards DNA profiles themselves, the Court notes that they contain a more limited amount of personal information extracted from cellular samples in a coded form. […]

75. The Court observes, nonetheless, that the profiles contain substantial amounts of unique personal data. While the information contained in the profiles may be considered objective and irrefutable in the sense submitted by the Government, their processing through automated means allows the authorities to go well beyond neutral identification. The Court notes in this regard that the Government accepted that DNA profiles could be, and indeed had in some cases been, used for familial searching with a view to identifying a possible genetic relationship between individuals. They also accepted the highly sensitive nature of such searching and the need for very strict controls in this respect. In the Court's view, the DNA profiles' capacity to provide a means of identifying genetic relationships between individuals (see paragraph 39 above) is in itself sufficient to conclude that their retention interferes with the right to the private life of the individuals concerned. The frequency of familial searches, the safeguards attached thereto and the likelihood of detriment in a particular case are immaterial in this respect (see *Amann*, cited above, § 69). This conclusion is similarly not affected by the fact that, since the information is in coded form, it is intelligible only with the use of computer technology and capable of being interpreted only by a limited number of persons.

76. The Court further notes that it is not disputed by the Government that the processing of DNA profiles allows the authorities to assess the likely ethnic origin of the donor and that such techniques are in fact used in police investigations (see paragraph 40 above). The possibility the DNA profiles create for inferences to be drawn as to ethnic origin makes their retention all the more sensitive and susceptible of affecting the right to private life. This conclusion is consistent with the principle laid down in the Data Protection Convention and reflected in the Data Protection Act that both list personal data revealing ethnic origin among the special categories of sensitive data attracting a heightened level of protection (see paragraphs 30-31 and 41 above).

77. In view of the foregoing, the Court concludes that the retention of both cellular samples and DNA profiles discloses an interference with the applicants' right to respect for their private lives, within the meaning of Article 8 § 1 of the Convention.

(ii) Fingerprints
78. It is common ground that fingerprints do not contain as much information as either cellular samples or DNA profiles. […]

79. In *McVeigh and Others*, the Commission first examined the issue of the taking and retention of fingerprints as part of a series of investigative measures. It accepted that at least some of the measures disclosed an interference with the applicants' private life, while leaving open the question of whether the retention of fingerprints alone would amount to such interference (see *McVeigh and Others v. the United Kingdom* (nos. 8022/77, 8025/77 and 8027/77, Commission's report of 18 March 1981, Decisions and Reports 25, p. 15, § 224).

80. In *Kinnunen*, the Commission considered that fingerprints and photographs retained following the applicant's arrest did not constitute an interference with his private life as they did not contain any subjective appreciations which called for refutation. The Commission noted, however, that the data at issue had been destroyed nine years later at the applicant's request (see *Kinnunen v. Finland*, no. 24950/94, Commission decision of 15 May 1996, unreported).

81. Having regard to these findings and the questions raised in the present case, the Court considers it appropriate to review this issue. It notes at the outset that the applicants' fingerprint records constitute their personal data (see paragraph 68 above) which contain certain external identification features much in the same way as, for example, personal photographs or voice samples.

82. In *Friedl*, the Commission considered that the retention of anonymous photographs that have been taken at a public demonstration did not interfere with the right to respect for private life. In so deciding, it attached special weight to the fact that the photographs concerned had not been entered in a data-processing system and that the authorities had taken no steps to identify the persons photographed by means of data processing (see *Friedl*, cited above, §§ 49-51).

83. In *P.G. and J.H. v. the United Kingdom*, the Court considered that the recording of data and the systematic or permanent nature of the record could give rise to private-life considerations even though the data in question may have been available in the public domain or otherwise. The Court noted that a permanent record of a person's voice for further analysis was of direct relevance to identifying that person when considered in conjunction with other personal data. It accordingly regarded the recording of the applicants' voices for such further analysis as amounting to interference with their right to respect for their private lives (see *P.G. and J.H. v. the United Kingdom*, no. 44787/98, §§ 59-60, ECHR 2001-IX).

84. […] fingerprints objectively contain unique information about the individual concerned, allowing his or her identification with precision in a wide range of circumstances. They are thus capable of affecting his or her private life and the retention of this information without the consent of the individual concerned cannot be regarded as neutral or insignificant.

85. The Court accordingly considers that the retention of fingerprints on the authorities' records in connection with an identified or identifiable individual may in itself give rise, notwithstanding their objective and irrefutable character, to important private-life concerns.

86. In the instant case, the Court notes furthermore that the applicants' fingerprints were initially taken in criminal proceedings and subsequently recorded on a national database with the aim of being permanently kept and regularly processed by automated means for criminal-identification purposes. It is accepted in this regard that, because of the information they contain, the retention of

cellular samples and DNA profiles has a more important impact on private life than the retention of fingerprints. However, the Court, like Baroness Hale (see paragraph 25 above), considers that, while it may be necessary to distinguish between the taking, use and storage of fingerprints, on the one hand, and samples and profiles, on the other, in determining the question of justification, the retention of fingerprints constitutes an interference with the right to respect for private life.

102. […] The breadth of [the margin of appreciation left to the national competent authorities] varies and depends on a number of factors, including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference. The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights (see Connors v. the United Kingdom, no. 66746/01, § 82, 27 May 2004, with further references). Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State will be restricted (see *Evans v. the United Kingdom* [GC], no. 6339/05, § 77, ECHR 2007-I). […]

103. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article (see, mutatis mutandis, *Z v. Finland*, cited above, § 95). The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored (see Article 5 of the Data Protection Convention and the Preamble thereto and Principle 7 of Recommendation No. R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector). The domestic law must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse (see notably Article 7 of the Data Protection Convention). The above considerations are especially valid as regards the protection of special categories of more sensitive data (see Article 6 of the Data Protection Convention) and more particularly of DNA information, which contains the person's genetic make-up of great importance to both the person concerned and his or her family (see Recommendation No. R (92) 1 of the Committee of Ministers on the use of analysis of DNA within the framework of the criminal justice system).

104. The interests of the data subjects and the community as a whole in protecting the personal data, including fingerprint and DNA information, may be outweighed by the legitimate interest in the prevention of crime (see Article 9 of the Data Protection Convention). However, the intrinsically private character of this information calls for the Court to exercise careful scrutiny of any State measure authorising its retention and use by the authorities without the consent of the person concerned (see, mutatis mutandis, *Z v. Finland*, cited above, § 96).

117. While neither the statistics nor the examples provided by the Government in themselves establish that the successful identification and prosecution of offenders could not have been achieved without the permanent and indiscriminate retention of the fingerprint and DNA records of all persons in the applicants' position, the Court accepts that the extension of the database has nonetheless contributed to the detection and prevention of crime.

118. The question, however, remains whether such retention is proportionate and strikes a fair balance between the competing public and private interests.

120. The Court acknowledges that the level of interference with the applicants' right to private life may be different for each of the three different categories of personal data retained. The retention of cellular samples is particularly intrusive given the wealth of genetic and health information contained therein. However, such an indiscriminate and open-ended retention regime as the one in issue calls

for careful scrutiny regardless of these differences.

121. […] The Court […] reiterates that the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having a direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data (see paragraph 67 above).

122. Of particular concern in the present context is the risk of stigmatisation, stemming from the fact that persons in the position of the applicants, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons. In this respect, the Court must bear in mind that the right of every person under the Convention to be presumed innocent includes the general rule that no suspicion regarding an accused's innocence may be voiced after his acquittal (see *Rushiti v. Austria*, no. 28389/95, § 31, 21 March 2000, with further references). It is true that the retention of the applicants' private data cannot be equated with the voicing of suspicions. Nonetheless, their perception that they are not being treated as innocent is heightened by the fact that their data are retained indefinitely in the same way as the data of convicted persons, while the data of those who have never been suspected of an offence are required to be destroyed.

124. The Court further considers that the retention of the unconvicted persons' data may be especially harmful in the case of minors such as the first applicant, given their special situation and the importance of their development and integration in society. The Court has already emphasised, drawing on the provisions of Article 40 of the United Nations Convention on the Rights of the Child of 1989, the special position of minors in the criminal-justice sphere and has noted, in particular, the need for the protection of their privacy at criminal trials (see *T. v. the United Kingdom* [GC], no. 24724/94, §§ 75 and 85, 16 December 1999). In the same way, the Court considers that particular attention should be paid to the protection of juveniles from any detriment that may result from the retention by the authorities of their private data following acquittals of a criminal offence. The Court shares the view of the Nuffield Council on Bioethics as to the impact on young persons of the indefinite retention of their DNA material and notes the Council's concerns that the policies applied have led to the over-representation in the database of young persons and ethnic minorities who have not been convicted of any crime (see paragraphs 38-40 above).

125. In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society. […]

***NG v Direktor na Glavna direktsia 'Natsionalna politsia' pri Ministerstvo na vatreshnite raboti – Sofia* (C-118/22), Judgment, Grand Chamber, Court of Justice of the European Union (30 January 2024)**

47. Next, Article 10 of Directive 2016/680 constitutes a specific provision governing the processing of special categories of personal data, including biometric and genetic data. The purpose of that article is to ensure enhanced protection of the data subject, since the data in question, because of their particular sensitivity and the context in which they are processed, are liable, as is apparent from recital 37 of that directive, to create significant risks to fundamental rights and freedoms, such as the right to respect for private life and the right to the protection of personal data, guaran teed by Articles 7 and 8 of the Charter (judgment of 26 January 2023, Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police), paragraph 116 and the case-law cited).

48. More specifically, Article 10 of Directive 2016/680 lays down the requirement that the processing

of sensitive data be allowed 'only where strictly necessary', which constitutes a strengthened condition for the lawful processing of such data and entails, inter alia, a particularly strict review of compliance with the principle of 'data minimisation', as derived from Article 4(1)(c) of Directive 2016/680; that requirement constitutes a specific application of that principle to those sensitive data (see, to that effect, judgment of 26 January 2023, Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police), C 205/21, EU:C:2023:49, paragraphs 117, 122 and 125).

50. It follows from Article 16(2) of Directive 2016/680 that that right to erasure may be exercised, inter alia, where the storage of the personal data in question is not or is no longer necessary for the purposes for which they are processed, in breach of the provisions of national law implementing Article 4(1)(c) and (e) of that directive and, as the case may be, Article 10 thereof, or where that erasure is required in order to comply with the time limit set, for that purpose, by national law pursuant to Article 5 of that directive.

SECTION 6: THE ROLE AND RESPONSIBILITIES OF COMPANIES IN SURVEILLANCE

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

Expressing concern that individuals, particularly children, often do not and/or cannot provide their free, explicit and informed consent to the collection, processing and storage of their data or to the reuse, sale or multiple resale of their personal data, as the collection, processing, use, storage and sharing of personal data, including sensitive data, have increased significantly in the digital age,

Emphasizing that States must respect international human rights obligations regarding the right to privacy when they intercept digital communications of individuals and/or collect personal data, when they share or otherwise provide access to data collected through, inter alia, information-and intelligence-sharing agreements and when they require disclosure of personal data from third parties, including private companies

Noting the increase in the collection of sensitive biometric information from individuals, and stressing that States must comply with their human rights obligations and that business enterprises should respect the right to privacy and other human rights when collecting, processing, sharing and storing biometric information by, inter alia, considering the adoption of data protection policies and safeguards,

7. *Calls upon* all States:

(h) To consider developing or maintaining and implementing legislation, regulations and policies to ensure that all business enterprises, including social media enterprises and other online platforms, fully respect the right to privacy and other relevant human rights in the design, development, deployment and evaluation of technologies, […]

(n) To refrain from requiring business enterprises to take steps that interfere with the right to privacy in an arbitrary or unlawful way;

(o) To protect individuals from violations or abuses of the right to privacy, including those which are caused by arbitrary or unlawful data collection, processing, storage and sharing, profiling and the use of automated processes and machine learning;

(p) To take steps to enable business enterprises to adopt adequate voluntary transparency measures with regard to requests by State authorities for access to private user data and information;

8. *Calls upon* all business enterprises, in particular those that collect, store, use, share and process data:

(b) To inform users in a clear, easily accessible and age-appropriate way about the collection, use, sharing and retention of their data that may affect their right to privacy, to refrain from doing so without their consent or a legal basis and to establish and to apply transparency policies that allow for the free, informed and meaningful consent of users, as appropriate;

(c) To implement administrative, technical and physical safeguards to ensure that data are processed lawfully and to ensure that such processing is limited to what is necessary in relation

to the purposes of the processing and that the legitimacy of such purposes, as well as the accuracy, integrity and confidentiality of the processing, is ensured;

(d) To ensure that respect for the right to privacy and other international human rights is incorporated into the design, operation, evaluation and regulation of automated decision-making and machine-learning technologies and to provide for compensation for the human rights abuses that they may cause or to which they may contribute;

(e) To ensure that individuals have access to their personal data and to adopt appropriate measures for the possibility to amend, correct, update, delete and withdraw consent for the data, in particular if the data are incorrect or inaccurate, or if the data were obtained illegally;

(f) To put in place adequate safeguards that seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services, including where necessary through contractual clauses or notification of any relevant entities of abuses or violations when misuse of their products and services is detected;

** See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016)*

UN General Assembly Resolution on Implementing the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms Through Providing a Safe and Enabling Environment for Human Rights Defenders and Ensuring Their Protection, UN Doc A/RES/74/146 (18 December 2019)

23. […] underlines the need to ensure human rights due diligence and the accountability of, and the provision of adequate remedies by, transnational corporations and other business enterprises, while also urging States to adopt relevant policies and laws in this regard, including to hold all companies to account for involvement in threats or attacks against human rights defenders;

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

Noting that the rapid pace of technological development enables individuals all over the world to use information and communications technology, and at the same time enhances the capacity of Governments, business enterprises and individuals to undertake surveillance, interception, hacking and data collection, which may violate or abuse human rights, in particular the right to privacy, and is therefore an issue of increasing concern,

Noting with deep concern also the use of technological tools developed by the private surveillance industry by private or public actors to undertake surveillance, hacking of devices and systems, including through the use of malware or spyware, interception and disruption of communications, and data collection, interfering with the professional and private lives of individuals, including those engaged in the promotion and defence of human rights and fundamental freedoms, journalists and other media workers, in violation or abuse of their human rights, specifically the right to privacy,

Recalling that business enterprises, including technology companies, have a responsibility to respect human rights, as set out in the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, and that the

obligation and the primary responsibility to promote and protect human rights and fundamental freedoms lie with the State, and welcoming the work of the Office of the High Commissioner on the application of these principles on digital technologies,

8. *Stresses* that States must comply with their human rights obligations and that business enterprises, including technology companies, should respect the right to privacy and other human rights when collecting, processing, sharing and storing personal data by, inter alia, adopting data protection policies and safeguards;

10. *Calls upon* all States:

(j) To consider adopting or reviewing legislation, regulations or policies to ensure that all business enterprises, including social media enterprises and other online platforms, fully incorporate the right to privacy and other relevant human rights into the design, development, deployment and evaluation of technologies, including artificial intelligence, to take appropriate steps to improve and encourage corporate accountability, and to provide individuals whose rights may have been violated or abused with access to an effective remedy, including reparation and guarantees of non-repetition;

(m) To provide effective and up-to-date guidance to business enterprises on how to respect human rights by advising on appropriate methods, including human rights due diligence, and on how to consider effectively issues of gender, vulnerability and/or marginalization, and to consider appropriate measures that would enable business enterprises to adopt adequate voluntary transparency measures with regard to requests by State authorities for access to private user data and information;

(p) To refrain from requiring business enterprises to take steps that interfere with the right to privacy in an arbitrary or unlawful way, and to protect individuals from harm, including that caused by business enterprises through data collection, processing, storage and sharing and profiling, and the use of automated processes and machine learning;

11. *Encourages* all business enterprises, in particular business enterprises that collect, store, use, share and process data:

(b) To inform users, in a clear and age-appropriate way that is easily accessible, including for persons with disabilities, about the collection, use, sharing and retention of their data that may affect their right to privacy, to refrain from doing so without their consent or a legal basis, and to establish transparency and policies that allow for the free, informed and meaningful consent of users;

(d) To implement administrative, technical and physical safeguards to ensure that data are processed lawfully, to ensure that such processing is necessary in relation to the purposes of the processing and that the legitimacy of such purposes, and the accuracy, integrity and confidentiality of the processing are ensured, and to prevent the unauthorized disclosure or use of data;

(e) To ensure that individuals have access to their data and the possibility to amend, correct, update, delete and withdraw consent for the use of their data, in particular if the data are incorrect or inaccurate or if the data were obtained illegally or used for discriminatory purposes;

(f) To ensure that respect for the right to privacy and other relevant human rights is incorporated into the design, operation, evaluation and regulation of automated decision-making and machine-learning technologies, and to provide effective remedies, including compensation, for human rights abuses that they have caused or to which they have contributed or been linked;

(g) To put in place adequate safeguards that seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services, including where necessary through contractual clauses, and to promptly inform relevant domestic, regional or international oversight bodies of abuses or violations when misuse of their products and services is detected;

(h) To enhance efforts to combat discrimination resulting from the use of artificial intelligence systems, including through human rights due diligence and monitoring and evaluation of artificial intelligence systems across their life cycle, and the human rights impact of their deployment;

12. *Encourages* business enterprises, including communications service providers, to work towards enabling solutions to secure and protect the confidentiality of digital communications and transactions, including measures for encryption, pseudonymization and anonymity, and to ensure the implementation of human-rights compliant safeguards, and calls upon States to promote measures and technical solutions for strong encryption, pseudonymization and anonymity, not to interfere with the use of such technical solutions, with any restrictions thereon complying with States' obligations under international human rights law, and to enact policies that protect the privacy of individuals' digital communications;

** See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/34/7 (23 March 2017); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/28/16 (26 March 2015)*

UN Human Rights Council Resolution on New and Emerging Digital Technologies and Human Rights, UN Doc A/HRC/RES/53/29 (14 July 2023)*

Noting that uses of new and emerging digital technologies that have an impact on the enjoyment of human rights may lack adequate regulation, and recognizing the need for effective measures to prevent, mitigate and remedy the adverse human rights impacts of such technologies in line with the obligations of States under international human rights law and the responsibilities of business enterprises under the Guiding Principles on Business and Human Rights, […]

Highlighting also the responsibility of business enterprises to respect human rights in line with the Guiding Principles on Business and Human Rights, including by implementing human rights due diligence policies and participating in good faith in domestic judicial and non-judicial processes,

3. *Highlights* the importance of the need to respect, protect and promote human rights and fundamental freedoms, in recognition of the inherent dignity of the human person, throughout the lifecycle of artificial intelligence systems and, towards this end, the need to pay particular attention to: […] (d) Ensuring that data for artificial intelligence systems are collected, used, shared, archived and deleted in ways that are consistent with States' respective obligations under international human rights law and the responsibilities of business enterprises in line with the Guiding Principles on Business and Human Rights;

** See also UN Human Rights Council Resolution on New and Emerging Digital Technologies and Human Rights, UN Doc UN Doc A/HRC/RES/47/23 (13 July 2021)*

Report of the United Nations High Commissioner for Human Rights, The right to Privacy in the Digital Age, UN Doc A/HRC/48/31 (13 September 2021)

48. States and businesses should ensure that comprehensive human rights due diligence is conducted when AI systems are acquired, developed, deployed and operated, as well as before big data held about individuals are shared or used. As well as resourcing and leading such processes, States may also require or otherwise incentivize companies to conduct comprehensive human rights due diligence. […]

60. The High Commissioner recommends that States and business enterprises: (a) Systematically conduct human rights due diligence throughout the life cycle of the AI systems they design, develop, deploy, sell, obtain or operate. A key element of their human rights due diligence should be regular, comprehensive human rights impact assessments […]"

Report of the United Nations High Commissioner for Human Rights, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests, UN Doc A/HRC/44/24 (24 June 2020)

39. The use of surveillance technologies has grown rapidly over recent years with the support of the private sector. All business enterprises, including those that develop new technologies that are used to monitor the activities of civil society actors, have a responsibility to respect human rights, […].

53. In this context, the High Commissioner recommends that States:

(j) Establish a moratorium on the use of facial recognition technology in the context of peaceful assemblies, at least until the authorities responsible can demonstrate compliance with privacy and data protection standards as well as the absence of significant accuracy issues and discriminatory impacts, and until the following recommendations are implemented:
(v) When relying on private companies to procure or deploy these facial recognition technologies, request that companies carry out human rights due diligence to identify, prevent, mitigate and address potential and actual adverse impact on human rights and, in particular, ensure that data protection and non-discrimination requirements be included in the design and the implementation of these technologies;

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

18. States often rely on business enterprises for the collection and interception of personal data. For example, some States compel telecommunications and Internet service providers to give them direct access to the data streams running through their networks. Such systems of direct access are of serious concern, as they are particularly prone to abuse and tend to circumvent key procedural safeguards. Some States also demand access to the massive amounts of information collected and stored by telecommunications and Internet service providers. States continue to impose mandatory obligations on telecommunications companies and Internet service providers to retain communications data for extended periods of time. Many such laws require the companies to collect and store indiscriminately all traffic data of all subscribers and users relating to all means of electronic communication. They limit people's ability to communicate anonymously, create the risk of abuses and may facilitate disclosure to third parties, including criminals, political opponents, or business competitors through hacking or other data breaches. Such laws exceed the limits of what can be considered necessary and proportionate. […]

36. In terms of its scope, the legal framework for surveillance should cover State requests to business enterprises. It should also cover access to information held extraterritorially or information-sharing with other States. A structure to ensure accountability and transparency

within governmental organizations carrying out surveillance needs to be clearly established in the law.

46. According to the Guiding Principles, all companies have a responsibility to undertake human rights due diligence to identify and address any human rights impacts of their activities. Taking a concrete example, companies selling surveillance technology should carry out, as part of their due diligence, a thorough human rights impact assessment prior to any potential transaction. Risk mitigation should include clear end-use assurances being stipulated in contractual agreements with strong human rights safeguards that prevent arbitrary or unlawful use of the technology and periodic reviews of the use of technology by States. Companies collecting and retaining user data need to assess the privacy risks connected to potential State requests for such data, including the legal and institutional environment of the States concerned. They must provide for adequate processes and safeguards to prevent and mitigate potential privacy and other human rights harms. Human rights impact assessments also need to be conducted, as part of the adoption of the terms of service and design and engineering choices that have implications for security and privacy, and decisions taken to provide or terminate services in a particular context (see A/HRC/32/38, para. 11).

47. […] In instances where national laws and regulations hinder such reporting, companies should use to the greatest extent possible any leverage they may have and are encouraged to advocate for the possibility to release such information.

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

34. […] where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obligations under the Covenant. If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation of those companies in that country, then human rights protections must be extended to those whose privacy is being interfered with, whether in the country of incorporation or beyond. This holds whether or not such an exercise of jurisdiction is lawful in the first place, or in fact violates another State's sovereignty.

Report of the Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, The Guiding Principles on Business and Human Rights: Guidance on Ensuring Respect for Human Rights Defenders, UN Doc A/HRC/47/39/Add.2 (22 June 2021)

22. […] The types of risks faced by human rights defenders when highlighting irresponsible practices involving business enterprises or their business partners (including actors with links to governments) include threats, or the reality, of: smears, slurs, harassment, intimidation, surveillance, strategic lawsuits against public participation (SLAPPs), criminalisation of their lawful activities, physical attacks and death.

50. Illustrative actions that States should take: […] provide guidance to business enterprises to assist them in trying to prevent their products or services with surveillance capabilities from being misused by others to commit human rights abuses.

104. States, business enterprises, and development finance institutions investing in and/or implementing development projects, may find themselves linked to, or complicit in human rights abuses targeting defenders due to engaging in, or reacting to, conflicts that target human rights defenders. For example, in order to facilitate business access to an area, or the advancement of a project. In other contexts, they may be involved in shutting down protests, conducting surveillance on defenders, or restricting trade union activity.

109. The use of products developed by technology companies, including in surveillance by business enterprises and by States, can severely restrict the rights of human rights defenders and endanger, and harm defenders themselves. All technology companies should resist any demands to restrict, or collude in restricting, human rights, especially the right to privacy, and the freedoms of expression, and of assembly and association. Human rights defenders ought not to be tracked or be put under surveillance when using the technology they rely on to do their work. They need to be supported in taking measures to protect themselves and business enterprises that understand and respect the work that human rights defenders do can play a vital role in sharing knowledge about the technology they have created.

110. Illustrative actions that technology companies should take: As feasible, technology companies should avoid Internet shutdowns and geo-blocking; Commit to the confidentiality of digital communications, including encryption and anonymity; […] remind States that seek to use business enterprises to surveil individuals that this may only be conducted on a targeted basis, and only when there is reasonable suspicion that someone is engaging, or planning to engage, in serious criminal offences, based on principles of necessity and proportionality, and with judicial supervision […]

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

28. It is clear from the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework adopted by the Human Rights Council in 2011, that a State's duty to protect includes a duty to take appropriate steps to prevent, investigate, punish and redress human rights abuse by third parties (A/HRC/17/31). In the Guiding Principles, States are urged to exercise adequate oversight in order to meet their international human rights obligations when they contract with, or legislate for, business enterprises to provide services that may have an impact on the enjoyment of human rights (ibid., p. 10).

30. The Guiding Principles provide a framework for assessing whether surveillance companies respect the rights of those affected by their products and services. In particular, there is an emphasis in the Guiding Principles on policy commitments to respect human rights; due diligence processes to identify, prevent, mitigate and account for human rights impacts; consultation with affected groups; ongoing evaluation of the effectiveness of human rights policies; and effective grievance mechanisms for affected rights holders (A/HRC/17/31, paras. 15–25).

31. By every measure, the companies would appear to fail to meet even these minimum baselines. The few companies that have published their customer policies gesture vaguely at the need to respect human rights. Hacking Team, for instance, states that it reviews "potential customers before a sale to determine whether or not there is objective evidence or credible concerns that Hacking Team technology provided to the customer will be used to facilitate human rights violations", but does not explain what it does with such information, or even identify which human rights its technologies might implicate. The NSO Group claims to operate in accordance with a Business Ethics Committee, "which includes outside experts from various disciplines, including law and foreign relations", and suggests that it may cancel work if its products are put to "improper use". On its website, it also states that it will "investigate any credible allegation of product misuse", but there is no indication of whether that includes human rights violations.

33. The guidance of the European Commission on implementing the Guiding Principles in the information and communications technology sector highlights the importance of "human rights by design". The extraordinary risk of the misuse of surveillance products means that companies should anticipate the illicit use of their software and begin engineering solutions for the inevitable negative impacts. In a promising move, the Government of the United Kingdom, in partnership

with a technology industry association, produced a set of guidelines for the cybersecurity industry in which they stress the importance of preventing and mitigating human rights risks "through appropriate design modification" at the earliest stages of product development.

48. Private companies are creating, transferring and servicing – and States are purchasing and using – surveillance technologies in troubling ways. Credible allegations have shown that companies are selling their tools to Governments that use them to target journalists, activists, opposition figures and others who play critical roles in democratic society. […]

67. For companies:

(a) Private surveillance companies should publicly affirm their responsibility to respect freedom of expression, privacy and related human rights, and integrate human rights due diligence processes from the earliest stages of product development and throughout their operations. These processes should establish human rights by design, regular consultations with civil society (particularly groups at risk of surveillance), and robust transparency reporting on business activities that have an impact on human rights;

(b) Companies should also put in place robust safeguards to ensure that any use of their products or services is compliant with human rights standards. These safeguards include contractual clauses that prohibit the customization, targeting, servicing or other use that violates international human rights law, technical design features to flag, prevent or mitigate misuse, and human rights audits and verification processes;

(c) When companies detect misuses of their products and services to commit human rights abuses, they should promptly report them to the relevant domestic, regional or international oversight bodies."

Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, UN Doc CCPR/C/ITA/CO/6 (28 March 2017)

36. [The Committee is concerned] about allegations that companies based in the State party have been providing on-line surveillance equipment to foreign governments with a record of serious human rights violations and the absence of legal safeguards or oversight mechanisms put in place in relation to such exports (art.17).

37. The State Party should […] take measures to ensure that all corporations under its jurisdiction, in particular technology corporations, respect human rights standards when engaging in operations abroad.

Annual Report of the Inter-American Commission on Human Rights 2020, Volume II – Annual Report of the Office of the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II Doc 28 (30 March 2021)

121. The growing role of the private sector in the surveillance activities of state security agencies must also be taken into consideration. The International Principles on the Application of Human Rights to Communications Surveillance call for the State to publish "aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each," and note that states should not interfere with service providers in their efforts to publish their procedures for assessing and complying with state requests, as well as other statistical information.

187. Security companies are playing an increasing role in communications surveillance activities

for national security purposes and in other state intelligence, military, and defense matters that have human rights implications. Various international bodies have issued statements on the responsibility of companies in the area of human rights. In 2011 the UN Human Rights Council adopted the Guiding Principles on Business and Human Rights which declare that while states are the primary holders of human rights obligations, corporations must also refrain from violating the human rights of third parties and must remedy violations in which they are directly or indirectly involved. In complying with these principles, businesses must undertake to prevent violations directly or indirectly related to their operations, products, or services and to mitigate the consequences even when they have not contributed to their creation.

189. Accordingly, i) states should ensure that access to public information laws are applied broadly and within the limits set out above to guarantee access to information about the management of public resources, the delivery of services, and the performance of public functions by non-state entities; ii) as part of the duty to protect, states should promote the responsibility of security sector companies with respect to human rights and conduct adequate oversight of companies' adherence to human rights laws, exercising the necessary regulatory powers; and iii) companies have a responsibility to disclose information that has an impact on the exercise of human rights.

UN General Assembly Resolution on Implementing the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms Through Providing a Safe and Enabling Environment for Human Rights Defenders and Ensuring Their Protection, UN Doc A/RES/74/146 (18 December 2019)

23. *Urges* non-State actors, including transnational corporations and other business enterprises, to assume their responsibility to respect the human rights and fundamental freedoms of all persons, including human rights defenders, and underlines the need to ensure human rights due diligence and the accountability of, and the provision of adequate remedies by, transnational corporations and other business enterprises, while also urging States to adopt relevant policies and laws in this regard, including to hold all companies to account for involvement in threats or attacks against human rights defenders;

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016)*

Noting also the increasing capabilities of business enterprises to collect, process and use personal data can pose a risk to the enjoyment of the right to privacy in the digital age,

Welcoming measures taken by business enterprises, on a voluntary basis, to provide transparency to their users about their policies regarding requests by State authorities for access to user data and information.

Recalling that business enterprises have a responsibility to respect human rights and that States must protect against human rights abuses, including of the right to privacy, within their territory and/or jurisdiction by third parties, including business enterprises, as set out in the Guiding Principles on business and Human rights: Implementing the United Nations "Protect, Respect and Remedy" Framework and in accordance with applicable laws and other international principles.

** See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014)*

UN Human Rights Council Resolution on Freedom of Opinion and Expression, UN Doc

A/HRC/RES/50/15 (8 July 2022)

11. *Encourages* business enterprises, including communications service providers, to work towards enabling solutions to secure and protect the confidentiality of digital communications and transactions, including measures for encryption, pseudonymization and anonymity, and to ensure the implementation of human rights-compliant safeguards, and calls upon States not to interfere with the use of such technical solutions with any restrictions thereon complying with States' obligations under international human rights law, and to enact policies that protect the privacy of individuals' digital communications;

Report of the Human Rights Council Advisory Committee, Possible Impacts, Opportunities and Challenges of New and Emerging Digital Technologies with Regard to the Promotion and Protection of Human Rights, UN Doc A/HRC/47/52 (19 May 2021)

19. Business and governance models that rely on user data are not easily reconciled with protecting individuals' right to privacy and minimizing the disclosure of personal data online. Although many engineers concede that there is a need for cybersecurity, new technologies and business models are purposely designed to collect, share and use personal data to influence consumers' purchasing decisions.

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

45. Where enterprises are faced with government demands for access to data that do not comply with international human rights standards, they are expected to seek to honour the principles of human rights to the greatest extent possible, and to be able to demonstrate their ongoing efforts to do so. This can mean interpreting government demands as narrowly as possible, seeking clarification from a Government with regard to the scope and legal foundation for the demand, requiring a court order before meeting government requests for data, and communicating transparently with users about risks and compliance with government demands. There are positive examples of industry action in this regard, both by individual enterprises and through multi-stakeholder initiatives.

46. A central part of human rights due diligence as defined by the Guiding Principles is meaningful consultation with affected stakeholders. In the context of information and communications technology companies, this also includes ensuring that users have meaningful transparency about how their data are being gathered, stored, used and potentially shared with others, so that they are able to raise concerns and make informed decisions. The Guiding Principles clarify that, where enterprises identify that they have caused or contributed to an adverse human rights impact, they have a responsibility to ensure remediation by providing remedy directly or cooperating with legitimate remedy processes. To enable remediation at the earliest possible stage, enterprises should establish operational-level grievance mechanisms.

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN Doc A/78/520 (10 October 2023)

33. The ubiquity of sophisticated communications surveillance poses obvious threats to civil society actors' and organizations' rights to privacy and free expression, as well as such related rights as the freedom of assembly and association and the freedom to manifest one's religion. Many global study respondents reported experiences of digital surveillance and the transfer of their private data […], leading to deep concerns among civil society about permissive surveillance and data-sharing arrangements, and a dearth of regulation and due diligence with respect to both States and private companies. The lack of regulation for private cybersecurity firms is profoundly concerning. The pernicious effect of unchecked and unregulated surveillance on civil society has been vividly demonstrated in the field of spyware. The position paper of the Special Rapporteur on the global regulation of the counter-terrorism spyware technology trade sets out in detail the inadequacy of the

existing regulatory regime and identifies the minimum features of a rights-respecting approach to the unique challenge of spyware.

Report of the Working Group on Enforced and Involuntary Disappearances, 'New technologies and enforced disappearances', UN Doc A/HRC/54/22/Add.5 (11 September 2023)

66. The Working Group recommends that technology and software corporations:

(d) Internet service providers, social media and related platforms should alert their users to Government hacking attempts and develop a guide for users of digital platforms, informing them on the risks of cyberattacks and theft and use of their data and metadata, sharing good practices to prevent such instances; they should also put in place robust guarantees to protect users' metadata from malicious exploitation;

(e) Surveillance corporations should take all necessary measures to abide by their international human rights obligations; in particular, they should exercise due diligence and carry out a thorough human rights impact assessment prior to any potential sale or transfer involving targeted and mass surveillance technologies, including facial-recognition, spyware and similar programmes; they should include contractual clauses that prohibit the use of surveillance technologies in violation of international human rights law and, upon detecting misuse, promptly report them to the relevant domestic, regional or international oversight bodies; and they should put in place remedial mechanisms that enable victims of abuses to submit complaints and seek redress;

(f) Contribute to the development of more secure means to collect, store and analyse data – especially sensitive information concerning disappeared persons and their relatives, ensuring its exclusively humanitarian use; and also develop open source and easily accessible tools to perform forensic analysis of potentially compromised electronic devices and digital spaces;

69. The Working Group recommends that other human rights mechanisms and international courts: (a) Promote accountability for States, corporations or individuals responsible for the misuse of targeted or mass surveillance technologies, as well as in cyberattacks, and, in general, in the use of new technologies to facilitate or conceal the commission of enforced disappearance;

Report of the Special Rapporteur on contemporary forms of slavery, including its causes and consequences, UN Doc A/78/161 (12 July 2023)

42. […] While States are primarily responsible for respecting and upholding the human rights standards on data protection, the Special Rapporteur is aware that an increasing number of private entities are engaging in collection, storage and analysis of available data in order to detect instances of contemporary forms of slavery. For those States without proper legislative or regulatory frameworks, there is a pressing need to ensure that the activities of these private entities also conform to the data protection and human rights standards with robust monitoring mechanisms in place. It should also be highlighted that the rules on data protection vary among Member States, despite initiatives such as the ISO 27701 standard of 2019 on privacy information management, adopted by the International Organization for Standardization. This makes cross-border cooperation such as intelligence exchange difficult. To address these and other issues, it may be necessary to promote a harmonization of data protection regimes among States and strengthen cooperation and collaboration with the proactive involvement of the technology sector.

49. Human rights due diligence in the technology sector should be strengthened. While mandatory and other forms of human rights due diligence are promoted by some Governments, technology companies of all sizes should also take human rights due diligence in their business activities more seriously by identifying and mitigating the risks of their tools and platforms being used to facilitate contemporary forms of slavery. Technological tools must also conform to the existing international human rights standards, including with regard to data protection and privacy.

51. The Special Rapporteur makes the following recommendations to technology companies: (k) Ensure robust data protection in handling collected data in line with the existing human rights and other standards; provide sufficient training to all employees, including subsidiaries and other partners; and work closely with States and civil society organizations in this regard;

Report of the Special Rapporteur on the Promotion and Protection of Human Rights while Counter-Terrorism, Human Rights Implications of the Development, Use, Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism, UN Doc A/HRC/52/39 (1 March 2023)

47. While in previous eras spycraft and surveillance technology tended to be the exclusive preserve of government agencies and in-house technical experts, in the modern era the vast majority of surveillance tools used by State agencies are obtained from the private sector. […] It is a matter of urgency that the activities of these businesses and multinational corporations be regulated, in line with the obligations of States with respect to the regulation of the business sector, to prevent human rights violations.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 'Reinforcing media freedom and the safety of journalists in the digital age', UN Doc A/HRC/50/29 (20 April 2022)

123. States should incorporate adequate safeguards in national laws, such as judicial oversight, to ensure that digital surveillance laws and activities do not undermine international standards on the protection of journalists and their sources. They should hold surveillance companies accountable for foreseeable use of their technology by their clients to target journalists, and amend sovereign immunity laws to permit civil action against States engaged in cross-border digital attacks on journalists.

124. Surveillance technology companies should publicly affirm their responsibility to respect human rights in line with the Guiding Principles on Business and Human Rights and Organization for Economic Cooperation and Development guidelines, and conduct and publicly disclose robust human rights due diligence for all proposed transfers of surveillance technology. They should refrain from exporting surveillance technology if there is a significant risk it will be used to commit human rights violations.

59. The Special Rapporteur emphasizes that:
(a) Business enterprises in new technology sectors must practically and publicly implement their operations guided by respect for international human rights law and act with due diligence so as to avoid adverse impacts on individuals and communities, including through the "respect, protect, remedy" framework set up under the Guiding Principles on Business and Human Rights;

(b) Business enterprises in new technology must conduct comprehensive human rights due diligence. This includes conducting risk assessments of actual and potential human rights impacts, both direct and indirect, during all phases of business operations;

(c) Businesses enterprises engaged in the development, use and transfer of high-risk new technologies must be subject to more stringent regulation and oversight by legislatures, courts and international regulation, including significant financial and administrative penalties for a failure to adopt adequate due diligence practices.

Report of the Working Group on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination, Impact of the Use of Private Military and Security Services in Immigration and Border Management on the Protection of the Rights of All Migrants, UN Doc A/HRC/45/9 (9 July 2020)

40. […] Companies have developed platforms that enable users to search across databases, allowing them to cross-reference data collected for different purposes. This push towards interoperability carries risks, for example, due to greater interactions between law enforcement and immigration databases. Among other things, immigration authorities have allegedly used this information to track, detain and deport migrants, including children.

Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, Racial Discrimination and Emerging Digital Technologies: a Human Rights Analysis, UN Doc A/HRC/44/57 (18 June 2020)

16. […] There are also concerns about the unregulated, and in some cases exploitative, terms on which data are extracted from individuals and nations in the global South, by profit-seeking corporate actors in the global North who cannot be held accountable.

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/43/52 (24 March 2020)

52. States and non-State actors should: (a) Protect the privacy of digital communications and enjoyment of the right to privacy by all individuals, regardless of their gender, by promoting tools such as encryption; (b) Ensure that restrictions to the right to privacy, including through mass or targeted surveillance, requests for personal data or limitations on the use of encryption, pseudonymity and anonymity tools: (i) Are on a case-specific basis; (ii) Do not discriminate on the basis of gender or other factors, such as indigeneity; (iii) Are reasonable, necessary and proportionate as required by law for a legitimate purpose and ordered only by a court.

Report of the Special Rapporteur on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination, UN Doc A/74/244 (29 July 2019)

23. […] Private military and security companies have been accused of surveillance and intimidation against human rights defenders, including women human rights defenders. […]

Report of the Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, Gender Dimensions of the Guiding Principles on Business and Human Rights, UN Doc A/HRC/41/43 (23 May 2019)

41. Business enterprises should communicate adequate and easily accessible information to the affected stakeholders regularly. Both the information and the means of communication should be responsive to gender discrimination and the differentiated impacts experienced by women.

42. Illustrative actions: (b) If the information communicated concerns sexual harassment and gender-based violence, business enterprises should respect the victims' right to privacy and should not disclose the identity or other personally identifiable information of victims to avoid social stigmatization and further victimization;

Report of the Special Rapporteur on the Situation of Human Rights Defenders, Situation of Women Human Rights Defenders, UN Doc A/HRC/40/60 (10 January 2019)

108. The Special Rapporteur recommends that Member States: […] (c) Ensure that non-State actors – including businesses, faith-based groups, the media and communities – meet their legal obligations to respect human rights. The Guiding Principles on Business and Human Rights are key for business enterprises;

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/32/38 (11 May 2016)

85. States bear a primary responsibility to protect and respect the right to exercise freedom of opinion and expression. In the information and communication technology context, this means that States must not require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extralegal means. Any demands, requests and other measures to take down digital content or access customer information must be based on validly enacted law, subject to external and independent oversight, and demonstrate a necessary and proportionate means of achieving one or more aims under article 19 (3) of the International Covenant on Civil and Political Rights. Particularly in the context of regulating the private sector, State laws and policies must be transparently adopted and implemented [...]

87. States place undeniable pressures on the private information and communication technology sector that often lead to serious restrictions on the freedom of expression. The private sector, however, also plays independent roles that may either advance or restrict rights, a point the Human Rights Council well understood by adopting the Guiding Principles on Business and Human Rights in 2011 as general guidance in that field. Private entities should be evaluated on the steps they take both to promote and undermine freedom of expression, even in hostile environments unfriendly to human rights.

88. Among the most important steps that private actors should take is the development and implementation of transparent human rights assessment procedures. They should develop and implement policies that take into account their potential impact on human rights. Such assessments should critically review the wide range of private sector activities in which they are engaged, such as the formulation and enforcement of terms of service and community standards on users' freedom of expression, including the outsourcing of such enforcement; the impact of products, services and other commercial initiatives on users' freedom of expression as they are being developed, including design and engineering choices, and plans for differential pricing of or access to Internet content and services; and the human rights impact of doing business with potential government customers, such as the operation of telecommunication infrastructure or the transfer of content-regulation or surveillance technologies.

89. It is also critical that private entities ensure the greatest possible transparency in their policies, standards and actions that implicate the freedom of expression and other fundamental rights. Human rights assessments should be subject to transparent review, in terms of their methodologies, their interpretation of legal obligations and the weight that such assessments have on business decisions. Transparency is important across the board, including in the context of content regulation, and should include the reporting of government requests for takedowns.

90. Beyond adoption of policies, private entities should also integrate commitments to freedom of expression into internal policymaking, product engineering, business development, staff training and other relevant internal processes.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/29/32 (22 May 2015)

60. […] Corporate actors should likewise consider their own policies that restrict encryption and anonymity (including through the use of pseudonyms).

62. While the present report does not draw conclusions about corporate responsibilities for communication security, it is nonetheless clear that, given the threats to freedom of expression online, corporate actors should review the adequacy of their practices with regard to human right norms. At a minimum, companies should adhere to principles such as those laid out in the Guiding Principles

on Business and Human Rights, the Global Network Initiative's Principles on Freedom of Expression and Privacy, the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, and the Telecommunications Industry Dialogue Guiding Principles. Companies, like States, should refrain from blocking or limiting the transmission of encrypted communications and permit anonymous communication. Attention should be given to efforts to expand the availability of encrypted data-centre links, support secure technologies for websites and develop widespread default end-to-end encryption. Corporate actors that supply technology to undermine encryption and anonymity should be especially transparent as to their products and customers."

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/23/40 (17 April 2013)

76. […] States should exercise adequate oversight in order to meet their international human rights obligations when they contract with, or legislate for, corporate actors where there may be an impact upon the enjoyment of human rights. Human rights obligations in this regard apply when corporate actors are operating abroad.

77. States must ensure that the private sector is able to carry out its functions independently in a manner that promotes individuals' human rights. At the same time, corporate actors cannot be allowed to participate in activities that infringe upon human rights, and States have a responsibility to hold companies accountable in this regard […].

95. States should ensure that communications data collected by corporate actors in the provision of communications services meets the highest standards of data protection.

96. States must refrain from forcing the private sector to implement measures compromising the privacy, security, and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption.

97. States must take measures to prevent the commercialization of surveillance technologies, paying particular attention to research, development, trade, export and use of these technologies considering their ability to facilitate systematic human rights violations.

Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, UN Doc CCPR/C/ITA/CO/6 (28 March 2017)

36. [The Committee is concerned] about allegations that companies based in the State party have been providing on-line surveillance equipment to foreign governments with a record of serious human rights violations and the absence of legal safeguards or oversight mechanisms put in place in relation to such exports (art.17).

37. The State Party should […] take measures to ensure that all corporations under its jurisdiction, in particular technology corporations, respect human rights standards when engaging in operations abroad.

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet OEA/Ser.L/V/II. CIDH/RELE/INF.11/13 (31 December 2013)

169. The service providers should be able to publicly disclose the procedures they use when they receive requests for information from government authorities, as well as information on at least the types of requests they receive and the number of requests. On this point, it bears noting that various Internet companies have adopted the practice of issuing transparency reports that disclose some aspects of the government requests for access to user information they receive […]

173. In the interest of controlling foreign surveillance of personal data, some States have proposed establishing a legal obligation of forced localization with respect to some intermediaries. Forced localization is understood as the legal obligation of the owners of Internet sites, platforms, and services to store the data or information on national users locally (in-country) if they provide their services in that country. The forced localization of data may be a mechanism for the restriction of freedom of expression for various reasons. First, the forced localization of Internet intermediaries substantially reduces the supply of services and platforms that users can freely access. It is important to note that the freedom to choose which services and platforms to access is a prerogative of users in the exercise of their freedom of expression and cannot be restricted by governments without violating the unique nature of the Internet as a free, open, and decentralized medium. This opportunity to choose is essential in many States in which individuals are subjected to arbitrary interference in their privacy bythe States. In such cases, the opportunity to choose the intermediaries that offer better security becomes a necessary condition for the uninhibited exercise of freedom of expression. In other words, the absence of adequate local laws or public policies for the protection of data could cause greater insecurity in the access to data if they are located in a specific country, as opposed to being stored in multiple locations or in places that offer better safeguards.

174. In addition, requiring Internet service providers to store data locally can create a barrier to entry into the market for new platforms and services. This would negatively affect the freedom of expression of users, who will see their access to resources for research, education, and communication reduced. Indeed, meeting the requirement of data localization is complex and costly, and harms individual users or new initiatives by potentially depriving them of the conditions of interoperability necessary to connect globally. Freedom of expression and democracy assume the free flow of information and require the prevention of measures that create fragmentation in the Internet.

SECTION 7: ACQUIRING AND SELLING SURVEILLANCE EQUIPMENT

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)*

Recognizing further the need to ensure that international human rights obligations are respected in the conception, design, development, deployment, evaluation and regulation of data-driven technologies and to ensure that they are subject to adequate safeguards and oversight, […]

6. *Acknowledges* that the conception, design, use, deployment and further development of new and emerging technologies, such as those that involve artificial intelligence, may have an impact on the enjoyment of the right to privacy and other human rights, and that the risks to these rights can and should be avoided and minimized by adapting or adopting adequate regulation or other appropriate mechanisms, in accordance with applicable obligations under international human rights law, for the conception, design, development and deployment of new and emerging technologies, including artificial intelligence, by taking measures to ensure a safe, transparent, accountable, secure and high quality data infrastructure and by developing human rights-based auditing mechanisms and redress mechanisms and establishing human oversight;

* See also *UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020)*

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)*

5. *Acknowledges* that risks to the right to privacy and other human rights can and should be minimized by adopting adequate regulations or other appropriate mechanisms, in accordance with applicable obligations under international human rights law, in the conception, design, use, acquisition, transfer, sale, deployment and further development of new and emerging digital technologies, such as artificial intelligence, by ensuring a safe, secure and high-quality data infrastructure, by exercising due diligence to assess, prevent and mitigate adverse human rights impacts, and by establishing human oversight, as well as redress mechanisms;

10. *Calls upon* all States: (n) To refrain from the use of surveillance technologies in a manner that is not compliant with international human rights obligations, including when used against human rights defenders, journalists and other media workers, and to take specific actions to protect against violations of the right to privacy, including by regulating the sale, transfer, use and export of surveillance technologies;

** See also UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021)*

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

19. Even if legitimate goals are being pursued, such as national security objectives or the protection of the rights of others, the assessment of the necessity and proportionality of the use of spyware severely limits the scenarios in which spyware would be permissible. […] OHCHR reiterates its recent call as well as those of human rights experts and groups for a moratorium on the sale, transfer and use of hacking tools until a human rights-based safeguards regime is in place.

56. […] OHCHR recommends that States:

(f) Promote public debate of the use of surveillance technologies and ensure meaningful participation of all stakeholders in decisions on the acquisition, transfer, sale, development, deployment and use of surveillance technologies, including the elaboration of public policies and their implementation;

(g) Implement moratoriums on the domestic and transnational sale and use of surveillance systems, such as hacking tools and biometric systems that can be used for the identification or classification of individuals in public places, until adequate safeguards to protect human rights are in place; such safeguards should include domestic and export control measures, in line with the recommendations made herein and in previous reports to the Human Rights Council;

57. […] OHCHR recommends that States: (f) Ensure that, in the provision and use of surveillance technologies, public-private partnerships uphold and expressly incorporate human rights standards and do not result in an abdication of governmental accountability for human rights.

Report of the United Nations High Commissioner for Human Rights, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests, UN Doc A/HRC/44/24 (24 June 2020)

40. […] States should refrain from granting export licences, if there are indications that the surveillance tools at issue could be used in the importing country to violate or abuse human rights. Against the background of widespread abuse of surveillance technologies around the world, the Special Rapporteur on the right to freedom of opinion and expression has called for States to impose a moratorium on granting export licences for surveillance technologies until the use of those technologies can be technically restricted to lawful purposes that are consistent with human rights standards, or until it can be ensured that those technologies will only be exported to countries in which their use is subject to authorization – granted in accordance with due process and the standards of legality, necessity and legitimacy – by an independent and impartial judicial body. The High Commissioner supports this call.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

34. Export controls are an important element of the effort to reduce the risks caused by the private surveillance industry and the repressive use of its tools. However, their effectiveness is limited. First, the relevant international export control regime – the non-binding Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, in which 42 States participate – is tailored to reduce threats to regional and international security. While that is a laudable and necessary objective, the framework is ill-suited to addressing the threats that targeted surveillance pose to human rights; indeed, it lacks guidelines or enforcement measures that would directly address human rights violations caused by surveillance tools. Second, the focus on exports is an imperfect proxy for addressing the central problem: the use of such technologies to target lawful expression, dissent, reporting and other examples of the exercise of human rights.

52. Judicial authorization of government use of surveillance technologies is necessary but insufficient. The purchase of these technologies should also be subject to meaningful public oversight, consultation and control. In recent years, as the use of surveillance technologies has proliferated among law enforcement bodies in the United States, several communities have instituted civilian control boards to regulate their use and purchase. The city of Oakland in California, for instance, adopted an ordinance with several features regarding the purchase of surveillance technology that could be replicated by States. These include:

(a) An approval process, carried out by the relevant departments, that takes into account the

State's human rights obligations;

(b) Public notice of such purchases through regular processes, and public consultations on issues such as the human rights implications of such purchases and whether the technologies at issue will be effective at achieving their intended purposes;

(c) Regular public reporting on such approvals, purchases and uses.

53. Particularly in States that allow subnational organs a certain autonomy in the purchase of law enforcement tools, community control of such purchases should be encouraged and enforced. Given the clear public interest in maintaining the privacy and security of widely available commercial software, public oversight mechanisms should also be empowered to set policies on the stockpiling of vulnerabilities and the development of relevant exploits."

55. States that are serious about the abuse of surveillance technologies should take steps to enable individual claims against both State and non-State actors. This will, for many States, necessarily involve ensuring that the rules concerning jurisdiction, evidence, timeliness and other basic threshold conditions are fit for purpose in the digital age. They should, for instance, ensure that courts can accept and evaluate as evidence the forensic analysis of technical experts. National legislation should also establish causes of action against private entities that take into account changes in corporate ownership (known as "disposals" or "makeovers"), which often complicate the efforts of victims to seek accountability and redress. Alternative forms of redress, such as truth commissions that enable victims of gross human rights abuses facilitated by digital surveillance to give testimony and that examine corporate complicity in these abuses, should also be considered.

58. In order to improve its role in developing global export standards, participating States would benefit from a human rights working group that could propose and consider standards for exports that integrate human rights concerns in technology transfers. […]

59. […] The [Wassenaar] Arrangement itself should promote such transparency by setting clear and enforceable guidelines for intergovernmental information-sharing and public disclosures concerning licensing standards, decisions to authorize, modify or reject licences, incidents or patterns of misuse of surveillance technologies and related human rights violations, and the treatment of digital vulnerabilities. National export laws should also allocate sufficient resources for public record-keeping and accessibility concerning export licensing decisions, and mandate relevant government agencies to solicit public input and conduct multi-stakeholder consultations when they are processing applications of export licences. Finally, States should also establish safe harbours for security research and exempt encryption items from export control restrictions.

60. Given the extraordinary risk of abuse of surveillance technologies, the granting of export licences should be prohibited under domestic law unless a company regularly demonstrates that it has rigorously implemented its responsibilities under the Guiding Principles with respect to the design, sale, transfer or support of such technologies. This would effectively establish the Guiding Principles as preconditions for companies to participate in the surveillance market. […]

66. For States:

(a) States should impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until a human rights-compliant safeguards regime is in place;

(b) States that purchase or use surveillance technologies ("purchasing States") should ensure that domestic laws permit their use only in accordance with the human rights standards of legality,

necessity and legitimacy of objectives, and establish legal mechanisms of redress consistent with their obligation to provide victims of surveillance-related abuses with an effective remedy;

(c) Purchasing States should also establish mechanisms that ensure public or community approval, oversight and control of the purchase of surveillance technologies;

(d) States that export or permit the export of surveillance technologies ("exporting States") should ensure that the relevant government agencies solicit public input and conduct multi-stakeholder consultations when they are processing applications for export licences. All records pertaining to export licences should be stored and made available to the greatest extent possible. They should also establish safe harbours for security research and exempt encryption items from export control restrictions;

(e) Exporting States should join the Wassenaar Arrangement and abide by its rules and standards to the extent that these are consistent with international human rights law;

(f) States participating in the Wassenaar Arrangement should develop a framework by which the licensing of any technology would be conditional upon a national human rights review and companies' compliance with the Guiding Principles on Business and Human Rights. Such a framework could be developed through a specially established human rights working group. Additionally, they should set clear and enforceable guidelines on transparency and accountability with respect to licensing decisions, surveillance-related human rights abuses and the treatment of digital vulnerabilities.

67. For companies:

(a) Private surveillance companies should publicly affirm their responsibility to respect freedom of expression, privacy and related human rights, and integrate human rights due diligence processes from the earliest stages of product development and throughout their operations. These processes should establish human rights by design, regular consultations with civil society (particularly groups at risk of surveillance), and robust transparency reporting on business activities that have an impact on human rights;

(b) Companies should also put in place robust safeguards to ensure that any use of their products or services is compliant with human rights standards. These safeguards include contractual clauses that prohibit the customization, targeting, servicing or other use that violates international human rights law, technical design features to flag, prevent or mitigate misuse, and human rights audits and verification processes;

(c) When companies detect misuses of their products and services to commit human rights abuses, they should promptly report them to the relevant domestic, regional or international oversight bodies. They should also establish effective grievance and remedial mechanisms that enable victims of surveillance-related human rights abuses to submit complaints and seek redress.

UN Human Rights Council Resolution on the Situation of Human Rights in Myanmar, UN Doc A/HRC/RES/52/31 (4 April 2023)*

7. *Calls upon* all States to respect their international commitments and all relevant United Nations resolutions and to cease the illicit transfer and diversion of arms, munitions and other military equipment to Myanmar, in order to prevent further violations of international humanitarian law and violations and abuses of human rights, as well as to refrain, in accordance with applicable national procedures and international norms and standards, from the export, sale or transfer of surveillance

goods and technologies and less-lethal weapons when they assess that there are reasonable grounds to suspect that such goods, technologies or weapons might be used to violate or abuse human rights, including in the context of assemblies;

** See also UN Human Rights Council Resolution on the Situation of human rights in Myanmar, UN Doc A/HRC/RES/49/23 (1 April 2022)*

UN Human Rights Council Resolution on the Promotion and protection of human rights in the context of peaceful protests, UN Doc A/HRC/RES/50/21 (8 July 2022)

30. *Calls upon* States to refrain, in accordance with applicable national procedures and international norms and standards, from the export, sale or transfer of surveillance goods and technologies and less-lethal weapons when they assess that there are reasonable grounds to suspect that such goods, technologies or weapons might be used to violate or abuse human rights, including in the context of assemblies;

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

25. The duty of States to protect against abuses of the right to privacy by companies and other third parties incorporated or domiciled within their jurisdiction has extraterritorial effects. For example, States should have in place export control regimes applicable to surveillance technology, which provide for assessing the legal framework governing the use of the technology in the destination country, the human rights record of the proposed end user and the safeguards and oversight procedures in place for the use of surveillance powers. Human rights guarantees need to be included in export licensing agreements.

Report of the Working Group on Enforced and Involuntary Disappearances, 'New technologies and enforced disappearances', UN Doc A/HRC/54/22/Add.5 (11 September 2023)

20. Spyware programmes can be acquired by Governments, mostly in a context that, in general, lacks independent oversight and sufficient regulation, especially with regard to import, export and use of such a technology. The Working Group learned with interest about the applicable legislation of certain States and existing regional regulations and international arrangements that are aimed at subjecting the sale and transfer of technologies to stricter control. While these are good practices, the applicable legal framework remains weak and fragmented and a thorough and independent scrutiny of the impact of these technologies on human rights should become the rule prior to their sale, transfer and use.

21. Instances where those – be they States, corporations or individuals – responsible for the misuse of surveillance technologies or abuses in their sale and transfer have been held to account are extremely rare. Until regulatory gaps are addressed in a comprehensive manner and corporations fully comply with their obligations under international law as spelled out pursuant to the Guiding Principles on Business and Human Rights, a moratorium on the sale, transfer and use of spyware should be enforced.

65. […] the Working Group recommends that States:

(g) Impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed targeted and mass surveillance tools, including spyware, facial-recognition and similar programmes, until a human rights-compliant safeguards regime is in place;

(h) Develop and enforce without delay a legal framework by which the licensing of any technology, and especially targeted and mass surveillance technologies, would be conditional upon a national human rights review and corporations' compliance with the Guiding Principles on Business and

Human Rights; the said framework must ensure that the transfer, sale and acquisition of targeted and mass surveillance technologies is subject to public consultation and oversight;

(i) Take all necessary measures to investigate, prosecute and hold accountable individuals, corporations and States responsible for human rights violations related to the sale, transfer and use of targeted and mass surveillance technologies;

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/23/40 (17 April 2013)

97. States must take measures to prevent the commercialization of surveillance technologies, paying particular attention to research, development, trade, export and use of these technologies considering their ability to facilitate systematic human rights violations.

Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, UN Doc CCPR/C/ITA/CO/6 (28 March 2017)

36. [The Committee is concerned] about allegations that companies based in the State party have been providing on-line surveillance equipment to foreign governments with a record of serious human rights violations and the absence of legal safeguards or oversight mechanisms put in place in relation to such exports (art.17).

LIST OF SOURCES

International Treaties and Agreements

American Convention on Human Rights (Pact of San Jose) (22 November 1969)

American Declaration on the Rights and Duties of Man (2 May 1948)

Arab Charter on Human Rights (22 May 2004)

Charter of Fundamental Rights of the European Union (7 December 2000)

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (28 January 1981)

Convention on the Rights of Persons with Disabilities (13 December 2006)

Convention on the Rights of the Child (20 November 1989)

Council of Europe Convention on Cybercrime (23 November 2001)

European Convention for the Protection of Human Rights and Fundamental Freedoms (4 November 1950)

International Convention on the Protection of the rights of All Migrant Workers and Members of Their Families (18 December 1990)

International Covenant on Civil and Political Rights (16 December 1966)

Organization for Economic Cooperation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980)

Universal Declaration of Human Rights (10 December 1948)

UN documents

UN General Assembly Documents

- **Resolutions**

UN General Assembly Resolution on Implementing the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms through Providing a Safe and Enabling Environment for Human Rights Defenders and Ensuring Their Protection, UN Doc A/RES/74/146 (18 December 2019)

UN General Assembly Resolution on Terrorism and Human Rights, UN Doc A/RES/74/147 (18 December 2019)

UN General Assembly Resolution on Terrorism and Human Rights, UN Doc A/RES/73/174 (17 December 2018)

UN General Assembly Resolution on Terrorism and Human Rights, UN Doc A/RES/78/210 (19 December 2023)

UN General Assembly Resolution on the Promotion and Protection of Human Right in the Context of Digital Technologies, UN Doc A/RES/78/213 (19 December 2023)

UN General Assembly Resolution on the Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc A/RES/72/180 (19 December 2017)

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022)

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020)

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018)

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/71/199 (19 December 2016)

UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014)

UN General Assembly Resolution on the Rights of the Children, UN Doc A/RES/78/187 (19 December 2023)

UN General Assembly Resolution on the Safety of **J**ournalists and the **I**ssue of **I**mpunity, UN Doc A/RES/78/215 (19 December 2023)

UN General Assembly Resolution on the Safety of Journalists and the Issue of Impunity, UN Doc A/RES/74/157 (18 December 2019)

UN General Assembly Resolution on the Safety of Journalists and the Issue of Impunity, UN Doc A/RES/72/175 (19 December 2017)

UN General Assembly Resolution on the Safety of Journalists and the Issue of Impunity, UN Doc A/RES/70/162 (17 December 2015)

UN General Assembly Resolution on the United Nations Global Counter-Terrorism Strategy: Eighth Review, UN Doc A/RES/77/298 (22 June 2023)

UN General Assembly Resolution on The United Nations Global Counter-Terrorism Strategy: Seventh Review, UN Doc A/RES/75/291 (30 June 2021)

- **Other**

Interim report of the Special Rapporteur on Freedom of Religion or Belief, 'Indigenous peoples and the right to freedom of religion or belief', UN Doc A/77/514 (10 October 2022)

Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, UN Doc A/75/590 (10 November 2020)

Report of the Special Rapporteur on Contemporary Forms of Slavery, including its Causes and Consequences, UN Doc A/78/161 (12 July 2023)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/78/520 (10 October 2023)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/75/261 (28 July 2020)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/71/373 (6 September 2016)

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/74/277 (5 August 2019)

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/71/368 (30 August 2016)

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, UN Doc A/75/184 (20 July 2020)

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, UN Doc A/74/349 (11 September 2019)

Report of the Special Rapporteur on the Situation of Human Rights Defenders, UN Doc A/74/159 (15 July 2019)

Report of the Special Rapporteur on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination, UN Doc A/74/244 (29 July 2019)

UN Human Rights Council Documents

- **Resolutions**

UN Human Rights Council Resolution on Civil Society Space, UN Doc A/HRC/RES/53/13 (13 July 2023)

UN Human Rights Council Resolution on Freedom of Opinion and Expression, UN Doc A/HRC/RES/50/15 (8 July 2022)

UN Human Rights Council Resolution on New and Emerging Digital Technologies and Human Rights, UN Doc A/HRC/RES/53/29 (14 July 2023)

UN Human Rights Council Resolution on New and Emerging Digital Technologies and Human Rights, UN Doc UN Doc A/HRC/RES/47/23 (13 July 2021)

UN Human Rights Council Resolution on Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/HRC/RES/35/34 (23 June 2017)

UN Human Rights Council Resolution on Recognizing the Contribution of Environmental Human Rights Defenders to the Enjoyment of Human Rights, Environmental Protection and Sustainable Development, UN Doc A/HRC/RES/40/11 (20 March 2019)

UN Human Rights Council Resolution on Terrorism and Human Rights, UN Doc A/HRC/RES/51/24 (7 October 2022)

UN Human Rights Council Resolution on the Freedom of Opinion and Expression, UN Doc

A/HRC/RES/44/12 (24 July 2020)

UN Human Rights Council Resolution on the Promotion and Protection of Human Rights in the Context of Peaceful Protests, UN Doc A/HRC/RES/50/21 (8 July 2022)

UN Human Rights Council Resolution on the Promotion and Protection of Human Rights in the Context of Peaceful Protests, UN Doc A/HRC/RES/44/20 (23 July 2020)

UN Human Rights Council Resolution on the Promotion and Protection of Human Rights in Nicaragua, UN Doc A/HRC/RES/49/3 (31 March 2022)

UN Human Rights Council Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, UN Doc A/HRC/RES/47/16 (13 July 2021)

UN Human Rights Council Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, UN Doc A/HRC/RES/38/7 (5 July 2018)

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023)

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021)

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019)

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/34/7 (23 March 2017)

UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/28/16 (26 March 2015)

UN Human Rights Council Resolution on the Rights to Freedom of Peaceful Assembly and of Association, UN Doc A/HRC/RES/50/17 (8 July 2022)

UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/45/18 (12 October 2020)

UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/39/6 (27 September 2018)

UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/33/2 (29 September 2016)

UN Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/54/21 (6 October 2022)

UN Human Rights Council Resolution on the Situation of Human Rights in Belarus in the Run-up to the 2020 Presidential Election and in its Aftermath, UN Doc A/HRC/RES/45/1 (21 September 2020)

UN Human Rights Council Resolution on the Situation of Human Rights in the Bolivarian Republic of Venezuela, UN Doc A/HRC/RES/42/25 (8 October 2019)

UN Human Rights Council Resolution on the Situation of human rights in the Russian Federation, UN Doc A/HRC/RES/54/23 (12 October 2023)

UN Human Rights Council Resolution on the Situation of Human Rights in Myanmar, UN Doc A/HRC/RES/52/31 (4 April 2023)

UN Human Rights Council Resolution on the Situation of human rights in Myanmar, UN Doc A/HRC/RES/49/23 (1 April 2022)

- **Other**

Report of the Human Rights Council Advisory Committee, Possible Impacts, Opportunities and Challenges of New and Emerging Digital Technologies with Regard to the Promotion and Protection of Human Rights, UN Doc A/HRC/47/52 (19 May 2021)

Report of the Independent Expert on the Protection Against Violence and Discrimination Based on Sexual Orientation and Gender Identity, Data Collection and Management as a Means to Create Heightened Awareness of Violence and Discrimination Based on Sexual Orientation and Gender Identity, UN Doc A/HRC/41/45 (14 May 2019)

Report of the Office of the United Nations High Commissioner for Human Rights, 'The practical application of the Guiding Principles on Business and Human Rights to the activities of technology companies', UN Doc A/HRC/50/56 (21 April 2022)

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014)

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022)

Report of the Secretary-General, Cooperation with the United Nations, its Representatives and Mechanisms in the Field of Human Rights, UN Doc A/HRC/48/24 (17 September 2021)

Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, Racial Discrimination and Emerging Digital Technologies: a Human Rights Analysis, UN Doc A/HRC/44/57 (18 June 2020)

Report of the Special Rapporteur on Freedom of Religion or Belief, UN Doc A/HRC/40/58 (5 March 2019)

Report of the Special Rapporteur on Freedom of Religion or Belief, Countering Islamophobia/Anti-Muslim Hatred to Eliminate Discrimination and Intolerance Based on Religion or Belief, UN Doc A/HRC/46/30 (13 April 2021)

Report of the Special Rapporteur on the Human Rights of Migrants, Right to Freedom of Association of Migrants and Their Defenders, UN Doc A/HRC/44/42 (13 May 2020)

Report of the Special Rapporteur on the Independence of Judges and Lawyers, 'Reimagining justice: confronting contemporary challenges to the independence of judges and lawyers', UN Doc A/HRC/53/31 (13 April 2023)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 'Reinforcing media freedom and the safety of journalists in the digital age', UN Doc A/HRC/50/29 (20 April 2022)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Disinformation and Freedom of Opinion and Expression, UN Doc A/HRC/47/25 (13 April 2021)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/32/38 (11 May 2016)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/29/32 (22 May 2015)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/23/40 (17 April 2013)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/20/17 (4 June 2012)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/17/27 (16 May 2011)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Impact of Measures to Address Terrorism and Violent Extremism on Civic Space and the Rights of Civil Society Actors and Human Rights Defenders, UN Doc A/HRC/40/52 (1 March 2019)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Human Rights Impact of Policies and Practices Aimed at Preventing and Countering Violent Extremism, UN Doc A/HRC/43/46 (21 February 2020)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Human Rights Impact of Counter-Terrorism and Countering (Violent) Extremism Policies and Practices on the Rights of Women, Girls and the Family, UN Doc A/HRC/46/36 (22 January 2021)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/HRC/13/37 (28 December 2009)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/HRC/34/61 (21 February 2017)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights while Counter-Terrorism, Human Rights Implications of the Development, Use, Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism, UN Doc A/HRC/52/39 (1 March 2023)

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/43/52 (24 March 2020)

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/40/63 (16 October 2019)

Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/31/64 (8 March 2016)

Report of the Special Rapporteur on the Right to Privacy: Artificial Intelligence and Privacy, and

Children's Privacy, UN Doc A/HRC/46/37 (25 January 2021)

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, UN Doc A/HRC/41/41 (17 May 2019)

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, Access to Justice as an Integral Element of the Protection of Rights to Freedom of Peaceful Assembly and Association, UN Doc A/HRC/47/24 (12 May 2021)

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association – Ten years protecting civic space worldwide, UN Doc A/HRC/44/50 (13 May 2020)

Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and Association, 'Protection of human rights in the context of peaceful protests during crisis situations', UN Doc A/HRC/50/42 (16 May 2022)

Report of the Special Rapporteur on the Situation of Human Rights Defenders, Situation of Women Human Rights Defenders, UN Doc A/HRC/40/60 (10 January 2019)

Report of the Special Rapporteur on the Situation of Human Rights Defenders, Human Rights Defenders Operating in Conflict and Post-conflict Situations, UN Doc A/HRC/43/51 (30 December 2019)

Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

Report of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/48/31 (13 September 2021)

Report of the United Nations High Commissioner for Human Rights, Promotion and Protection of the Human Rights and Fundamental Freedoms of Africans and of People of African Descent Against Excessive Use of Force and Other Human Rights Violations by Law Enforcement Officers, UN Doc A/HRC/47/53 (1 June 2021)

Report of the United Nations High Commissioner for Human Rights, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests, UN Doc A/HRC/44/24 (24 June 2020)

Report of the United Nations High Commissioner for Human Rights, Summary of consultations on enhancing access to remedy in the technology sector and on the enforcement of human rights due diligence, UN Doc A/HRC/50/45/Add.1 (1 June 2022)

Report of the Working Group of Experts on People of African Descent on its Twenty-Third and Twenty-Fourth Sessions, UN Doc A/HRC/42/59 (15 August 2019)

Report of the Working Group on Discrimination Against Women and Girls, Women's and Girls' Sexual and Reproductive Health Rights in Crisis, UN Doc A/HRC/47/38 (28 April 2021)

Report of the Working Group on Enforced and Involuntary Disappearances, 'New technologies and enforced disappearances', UN Doc A/HRC/54/22/Add.5 (11 September 2023)

Report of the Working Group on Enforced and Involuntary Disappearances, UN Doc A/HRC/54/22 (8 August 2023)

Report of the Working Group on the Issue of Human Rights and Transnational Corporations and

Other Business Enterprises, The Guiding Principles on Business and Human Rights: Guidance on Ensuring Respect for Human Rights Defenders, UN Doc A/HRC/47/39/Add.2 (22 June 2021)

Report of the Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, Gender Dimensions of the Guiding Principles on Business and Human Rights, UN Doc A/HRC/41/43 (23 May 2019)

Report of the Working Group on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination, Impact of the Use of Private Military and Security Services in Immigration and Border Management on the Protection of the Rights of All Migrants, UN Doc A/HRC/45/9 (9 July 2020)

UN Treaty Bodies

UN Human Rights Committee Documents

Antonius Cornelis Van Hulst v Netherlands, Comm No 903/1999, Human Rights Committee, UN Doc CCPR/C/82/D903/1999 (15 November 2004)

Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, UN Doc CCPR/C/USA/CO/4 (23 April 2014)

Concluding Observations on Equatorial Guinea in the Absence of its Initial Report, Human Rights Committee, UN Doc CCPR/C/GNQ/CO/1 (22 August 2019)

Concluding Observations on Nigeria in the Absence of its Second Periodic Report, Human Rights Committee, UN Doc CCPR/C/NGA/CO/2 (29 August 2019)

Concluding Observations on the Eighth Periodic Report of Colombia, UN Doc CCPR/C/COL/CO/8 (21 July 2023)

Concluding Observations on the Eighth Periodic Report of the Russian Federation, Human Rights Committee, UN Doc CCPR/C/RUS/CO/8 (1 November 2022)

Concluding Observations on the Eighth Periodic Report of Ukraine, UN Doc CCPR/C/UKR/CO/8 (11 November 2021)

Concluding Observations on the Eighth Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/8 (26 March 2024)

Concluding Observations on the Fifth Periodic Report of Belarus, Human Rights Committee, UN Doc CCPR/C/BLR/CO/5 (22 November 2018)

Concluding Observations on the Fifth Periodic Report of France, Human Rights Committee, UN Doc CCPR/C/FRA/CO/5 (17 August 2015)

Concluding Observations on the Fifth Periodic Report of Ireland, Human Rights Committee, UN Doc CCPR/C/IRL/CO/5 (22 July 2022)

Concluding Observations on the Fifth Periodic Report of Sri Lanka, Human Rights Committee, UN Doc CCPR/C/LKA/CO/5 (21 November 2014)

Concluding Observations on the Fifth Periodic Report of the Netherlands, Human Rights Committee, UN Doc CCPR/C/NLD/CO/5 (22 August 2019)

Concluding Observations on the Fifth Periodic Report of the Philippines, Human Rights Committee, UN Doc CCPR/C/PHL/CO/5 (28 October 2022)

Concluding Observations on the Fifth Periodic Report of the Republic of Korea, Human Rights Committee, UN Doc CCPR/C/KOR/CO/5 (30 October 2023)

Concluding Observations on the Fifth Periodic Report of the United States of America, Human Rights Committee, UN Doc CCPR/C/USA/CO/5 (30 October 2023)

Concluding Observations on the Fourth Periodic Report of Bulgaria, Human Rights Committee, UN Doc CCPR/C/BGR/CO/4 (15 November 2018)

Concluding Observations on the Fourth Periodic Report of Estonia, Human Rights Committee, UN Doc CCPR/C/EST/CO/4 (18 April 2019)

Concluding Observations on the Fourth Periodic Report of Hong Kong, China, Human Rights Committee, UN Doc CCPR/C/CHN-HKG/CO/4 (22 July 2022)

Concluding Observations on the Fourth Periodic Report of Nicaragua, Human Rights Committee, UN Doc CCPR/C/NIC/CO/4 (31 October 2022)

Concluding Observations on the Fourth Periodic Report of Paraguay, Human Rights Committee, UN Doc CCPR/C/PRY/CO/4 (20 August 2019)

Concluding Observations on the Fourth Periodic Report of Rwanda, Human Rights Committee, UN Doc CCPR/C/RWA/CO/4 (2 May 2016)

Concluding Observations on the Fourth Periodic Report of Switzerland, Human Rights Committee, UN Doc CCPR/C/CHE/CO/4 (27 July 2017) (translated from the original French)

Concluding Observations on the Fourth Periodic Report of the Islamic Republic of Iran, Human Rights Committee, UN Doc CCPR/C/IRN/CO/4 (26 October 2023)

Concluding Observations on the Fourth Periodic Report of the Republic of Korea, Human Rights Committee, UN Doc CCPR/C/KOR/CO/4 (3 December 2015)

Concluding Observations on the Fourth Periodic Report of Serbia, Human Rights Committee, UN Doc CCPR/C/SRB/CO/4 (26 March 2024)

Concluding Observations on the Fourth Periodic Report of Zambia, Human Rights Committee, UN Doc CCPR/C/ZMB/CO/4 (20 March 2023)

Concluding Observations on the Initial Periodic Report of Malawi, Human Rights Committee, UN Doc CCPR/C/MWI/CO/1/Add.1 (19 August 2014)

Concluding Observations on the Initial Report of Pakistan, Human Rights Committee, UN Doc CCPR/C/PAK/CO/1 (27 July 2017)

Concluding Observations on the Initial Report of South Africa, Human Rights Committee, UN Doc CCPR/C/ZAF/CO/1 (27 April 2016)

Concluding Observations on the Initial Report of the State of Palestine, UN Doc CCPR/C/PSE/CO/1 (21 July 2023)

Concluding Observations on the Second Periodic Report of Botswana, Human Rights Committee, UN Doc CCPR/C/BWA/CO/2 (11 November 2021)

Concluding Observations on the Second Periodic Report of Honduras, Human Rights Committee, UN Doc CCPR/C/HND/CO/2 (27 July 2017) (translated from the original Spanish)

Concluding Observations on the Second Periodic Report of Indonesia, Human Rights Committee, UN Doc CCPR/C/IDN/CO/2 (26 March 2024)

Concluding Observations on the Second Periodic Report of Lesotho, UN Doc CCPR/C/LSO/CO/2 (21 July 2023)

Concluding Observations on the Second Periodic Report of Namibia, Human Rights Committee, UN Doc CCPR/C/NAM/CO/2 (22 April 2016)

Concluding Observations on the Second Periodic Report of Turkmenistan, Human Rights Committee, UN Doc CCPR/C/TKM/CO/2 (28 March 2017)

Concluding Observations on the Second Periodic Report of Uganda, Human Rights Committee, UN Doc CCPR/C/UGA/CO/2 (20 July 2023)

Concluding Observations on the Seventh Periodic Report of Colombia, Human Rights Committee, UN Doc CCPR/COL/CO/4 (4 November 2016)

Concluding Observations on the Seventh Periodic Report of Finland, Human Rights Committee, UN Doc CCPR/C/FIN/CO/7 (3 May 2021)

Concluding Observations on the Seventh Periodic Report of Germany, Human Rights Committee, UN Doc CCPR/C/DEU/CO/7 (11 November 2021)

Concluding Observations on the Seventh Periodic Report of Japan, Human Rights Committee, UN Doc CCPR/C/JPN/CO/7 (28 October 2022)

Concluding Observations on the Seventh Periodic Report of Norway, Human Rights Committee, UN Doc CCPR/C/NOR/CO/7 (25 April 2018)

Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee, UN Doc CCPR/C/POL/CO/7 (4 November 2016)

Concluding Observations on the Seventh Periodic Report of Sweden, Human Rights Committee, UN Doc CCPR/C/SWE/CO/7 (28 April 2016)

Concluding Observations on the Seventh Periodic Report of the Russian Federation, Human Rights Committee, UN Doc CCPR/C/RUS/CO/7 (28 April 2015)

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, UN Doc CCPR/C/GBR/CO/7 (17 August 2015)

Concluding Observations on the Sixth Periodic Report of Belgium, Human Rights Committee, UN Doc CCPR/C/BEL/CO/6 (6 December 2019)

Concluding Observations on the Sixth Periodic Report of Canada, Human Rights Committee, UN Doc CCPR/C/CAN/CO/6 (13 August 2015)

Concluding Observations on the Sixth Periodic Report of Denmark, Human Rights Committee, UN

Doc CCPR/C/DNK/CO/6 (15 August 2016)

Concluding Observations on the Sixth Periodic Report of Hungary, Human Rights Committee, UN Doc CCPR/C/HUN/CO/6 (9 May 2018)

Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, UN Doc CCPR/C/ITA/CO/6 (28 March 2017)

Concluding Observations on the Sixth Periodic Report of Morocco, Human Rights Committee, UN Doc CCPR/C/MAR/CO/6 (4 November 2016)

Concluding Observations on the Sixth Periodic Report of New Zealand, Human Rights Committee, UN Doc CCPR/C/NZL/CO/6 (28 April 2016)

Concluding Observations on the Sixth Periodic Report of Sri Lanka, Human Rights Committee, UN Doc CCPR/C/LKA/CO/6 (21 March 2023)

Concluding Observations on the Third Periodic Report of Brazil, Human Rights Committee, UN Doc CCPR/C/BRA/CO/3 (20 July 2023)

Concluding Observations on the Third Periodic Report of Kuwait, Human Rights Committee, UN Doc CCPR/C/KWT/CO/3 (11 August 2016)

Concluding Observations on the Third Periodic Report of Lebanon, Human Rights Committee, UN Doc CCPR/C/LBN/CO/3 (9 May 2018)

Concluding Observations on the Third Periodic Report of Tajikistan, Human Rights Committee, UN Doc CCPR/C/TJK/CO/3 (22 August 2019)

Concluding Observations on the Third Periodic Report of the Former Yugoslav Republic of Macedonia, Human Rights Committee, UN Doc CCPR/C/MKD/CO/3 (17 August 2015)

Concluding Observations on the Third Periodic Report of Namibia, Human Rights Committee, UN Doc CCPR/C/NAM/CO/3 (22 March 2024)

Concluding Observations on the Third Periodic Report of Turkmenistan, UN Doc CCPR/C/TKM/CO/3 (17 March 2023)

Toonen v Australia, Comm No 488/1992, Human Rights Committee, UN Doc CCPR/C/50/D/488/1992 (31 March 1994)

UN Human Rights Committee, General Comment No 16: Article 17 (Right to Privacy), UN Doc HRI/GEN/1/Rev.1 (8 April 1988)

UN Human Rights Committee, General Comment No 37 (2020) on the Right of Peaceful Assembly (Article 21), UN Doc CCPR/C/GC/37 (17 September 2020)

Other

Committee on the Elimination of Racial Discrimination, General Recommendation No 36 (2020) on Preventing and Combating Racial Profiling by Law Enforcement Officials, UN Doc CERD/C/GC/36 (17 December 2020)

European Law

European Court of Human Rights Case Law

Akhlyustin v Russia, App No 21200/05, Judgment, European Court of Human Rights (7 November 2017)

Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria, App No 62540/00, Judgment, European Court of Human Rights (28 June 2007)

Aycaguer v France, App No 8806/12, Judgment, European Court of Human Rights (22 June 2017)

Azer Ahmadov v Azerbaijan, App No 3409/10, Judgment, European Court of Human Rights (22 July 2021)

Ben Faiza v France, App No 31446/12, Judgment, European Court of Human Rights (8 February 2018) (translated from the original French)

Benedik v Slovenia, App No 62357/14, Judgment, European Court of Human Rights (24 April 2018)

Berlizev v Ukraine, App No 43571/12, Judgment, European Court of Human Rights (8 July 2021)

Big Brother Watch and Others v The United Kingdom, Apps Nos 58170/13, 62322/14 and 24960/15, Grand Chamber, Judgment, European Court of Human Rights (25 May 2021)

Bosak and Others v Croatia, Apps Nos 40429/14 and 3 others, Judgment, European Court of Human Rights (6 June 2019)

Breyer v Germany, App No 50001/12, Judgment, European Court of Human Rights (30 January 2020)

Bykov v Russia, App No 4378/02, Judgment, Grand Chamber, European Court of Human Rights (10 March 2009)

Catt v The United Kingdom, App No 43514/15, Judgment, European Court of Human Rights (24 January 2019)

Centrum för Rättvisa v Sweden, App No 35252/08, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021)

Dragojević v Croatia, App No 68955/11, Judgment, European Court of Human Rights (15 January 2015)

Dudchenko v Russia, App No 37717/05, Judgment, European Court of Human Rights (7 November 2017)

Ekimdzhiev and Ors v Bulgaria, App No 70078/12, Judgment, European Court of Human Rights (11 January 2022)

Eminağaoğlu v Turkey, App No 76521/1, Judgment, European Court of Human Rights (9 March 2021)

Gaughran v The United Kingdom, App No 45245/15, Judgment, European Court of Human Rights (13 February 2020)

Glukhin v Russia, App No 11519/20, Judgment, European Court of Human Rights (04 July 2023)

Gorlov and Others v Russia, Apps Nos 27057/06 and 2 others, Judgment, European Court of Human Rights (2 July 2019)

Hambardzumyan v Armenia, App No 43478/11, Judgment, European Court of Human Rights (5 December 2019)

Haščak v Slovakia, Apps Nos 58359/12 and 2 others, Judgment, European Court of Human Rights (23 June 2022)

Iordachi and Others v Moldova, App No 25198/02, Judgment, European Court of Human Rights (10 February 2009)

Ivashchenko v Russia, App No 61064/10, Judgment, European Court of Human Rights (13 February 2018)

Kaczmarek v Poland, App No 16974/14, Judgment, European Court of Human Rights (22 February 2024)

Kadura and Smaliy v Ukraine, Apps Nos 42753/14 and 43860/14, Judgment, European Court of Human Rights (21 January 2021)

Kennedy v The United Kingdom, App No 26839/05, Judgment, European Court of Human Rights (18 May 2010)

Khadija Ismayilova v Azerbaijan, Apps Nos 65286/13 and 57270/14, Judgment, European Court of Human Rights (10 January 2019)

Klass and Others v Germany, App No 5029/71, Judgment, European Court of Human Rights (6 September 1978)

Konstantin Moskalev v Russia, App No 59589/10, Judgment, European Court of Human Rights (7 November 2017)

Kopp v Switzerland, App No 23224/94, Judgment, European Court of Human Rights (25 March 1998)

Kruglov and Others v Russia, Apps Nos 11264/04 and 15 others, Judgment, European Court of Human Rights (4 February 2020)

Kruslin v France, App No 11801/85, Judgment, European Court of Human Rights (24 April 1990)

Leander v Sweden, App No 9248/81, Judgment, European Court of Human Rights (26 March 1987)

Liberty and Others v The United Kingdom, App No 58243/00, Judgment, European Court of Human Rights (1 July 2008)

Liblik and Others v Estonia, Apps Nos 173/15 and 5 others, Judgment, European Court of Human Rights (28 May 2019)

Malone v The United Kingdom, App No 8691/79, Judgment, European Court of Human Rights (2 August 1984)

N.F. and Others v Russia, Apps Nos 3537/15 and 8 others, Judgment, European Court of Human Rights (12 September 2023)

Nuh Uzun and Others v Türkiye, App No 49341/18 and 13 others, Judgment, European Court of Human Rights (29 March 2022)

P.N. v Germany, App No 74440/17, Judgment, European Court of Human Rights (11 June 2020)

Plechlo v Slovakia, App No 18593/19, Judgment, European Court of Human Rights (26 October 2023)

Potoczká and Adamčo v Slovakia, App No 7286/16, Judgment, European Court of Human Rights (12 January 2023)

Roman Zakharov v Russia, App No 47143/06, Judgment, European Court of Human Rights (4 December 2015)

Rotaru v Romania, App No 28341/95, Judgment, European Court of Human Rights (4 May 2000)

S. and Marper v The United Kingdom, Apps Nos 30562/04 and 30566/04, Judgment, European Court of Human Rights (4 December 2008)

Saber v Norway, App No 459/18, Judgment, European Court of Human Rights (17 December 2020)

Särgava v Estonia, App No 698/19, Judgment, European Court of Human Rights (16 November 2021)

Sedletska v Ukraine, App No 42634/18, Judgment, European Court of Human Rights (1 April 2021)

Shimovolos v Russia, App No 30194/09, Judgment, European Court of Human Rights (21 June 2011)

Škoberne v Slovenia, App No 19920/20, Judgment, European Court of Human Rights (15 February 2024)

Sommer v Germany, App No 73607/13, Judgment, European Court of Human Rights (27 April 2017)

Svetova and Others v Russia, App No 54714/17, Judgment, European Court of Human Rights (24 January 2023)

Szabó and Vissy v Hungary, App No 37138/14, Judgment, European Court of Human Rights (12 January 2016)

Taylor-Sabori v The United Kingdom, App No 47114/99, Judgment, European Court of Human Rights (22 October 2002)

Trajkovski and Chipovski v North Macedonia, Apps Nos 53205/13 and 63320/13, Judgment, European Court of Human Rights (13 February 2020)

Uzun v Germany, App No 35623/05, Judgment, European Court of Human Rights (2 September 2010)

Vasil Vasilev v Bulgaria, App No 7610/15, Judgment, European Court of Human Rights (16 November 2021)

Weber and Saravia v Germany, App No 54934/00, Decision, European Court of Human Rights (29 June 2006)

Wieder and Guarnieri v the United Kingdom, Apps Nos 64371/16 and 64407/16, Judgment, European Court of Human Rights (12 September 2023)

Yunusova and Yunusov v Azerbaijan (No 2), App No 68817/14, Judgment, European Court of Human Rights (16 July 2020)

Zoltán Varga v Slovakia, App No 58361/12 and 2 others, Judgment, European Court of Human Rights (20 July 2021)

Zubkov and others v Russia, App No 29431/05 and 2 others, Judgment, European Court of Human Rights (7 November 2017)

Council of Europe

Commissioner for Human Rights, Council of Europe, Issue Paper on Democratic and Effective Oversight of National and Security Services (May 2015)

Commissioner for Human Rights, Council of Europe, Positions on Counter-Terrorism and Human Rights Protection CommDH/PositionPaper(2015)1 (5 June 2015)

Council of Europe Convention on Cybercrime, Preamble (23 November 2001)

Inter-American Law

Inter-American Court of Human Rights

Escher et al. v Brazil, Inter-American Court of Human Rights, Judgment (on Preliminary Objection, Merits, Reparations, and Costs), Series C No 200 (6 July 2009)

Garcia v Peru, Inter-American Court of Human Rights, Case 11.006, Report No 1/95, OEA/Ser.L/V/II.88 (17 February 1995)

Tristán Donoso v Panamá, Inter-American Court of Human Rights, Judgment (on Preliminary Objection, Merits, Reparations, and Costs), Series C No 193 (27 January 2009)

Inter-American Commission on Human Rights

Annual Report of the Inter-American Commission on Human Rights 2020, Volume II – Annual Report of the Office of the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II Doc 28 (30 March 2021)

Annual Report of the Inter-American Commission on Human Rights 2019, Volume II – Annual Report of the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II. Doc 5 (24 February 2020)

Ms. X and Y v Argentina, Inter-American Commission on Human Rights, Case 10.506, Report No 38/96 (15 October 1996)

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission

on Human Rights, Concern Over the Acquisition and Implementation of Surveillance Programs by States of the Hemisphere, Press Release R80/15 (21 July 2015)

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet OEA/Ser.L/V/II. CIDH/RELE/INF.11/13 (31 December 2013)

African Law

African Commission on Human and Peoples' Rights

African Commission on Human and Peoples' Rights, Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa, ACHPR/Res.573 (LXXVII) (9 November 2023)

African Commission on Human and Peoples' Rights, Resolution on the Protection of Women Against Digital Violence in Africa, ACHPR/Res. 522 (LXXII) (11 August 2022)

Commissioner Lawrence M. Mute, Vice-Chairperson of the African Commission on Human and Peoples' Rights and Special Rapporteur on Freedom of Expression and Access to Information in Africa, 65th Ordinary Session of the African Commission on Human and Peoples' Rights (21 October - 10 November 2019)

EU Law

Court of Justice of the European Union Case Law

Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH (C 793/19 and C 794/19), Judgment, Grand Chamber, Court of Justice of the European Union (20 September 2022)

Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems (C-311/18), Judgment, Grand Chamber, Court of Justice of the European Union (16 July 2020)

Digital Rights Ireland Ltd v Minister of Communications, Marine and Natural Resources et al. (C-293/12*); Kärntner Landesregierung and others* (C-594/12), Joined Cases, Judgment, Grand Chamber, Court of Justice of the European Union (8 April 2014)

G.D. v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, and Attorney General, (C-140/20), Judgment, Grand Chamber, Court of Justice of the European Union (5 April 2022)

La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net v Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées; Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministers (C-511/18, C-512/18 and C-520/18), Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2020)

Ligue des droits humains v Conseil des ministres (C-817/19), Judgment, Grand Chamber, Court of Justice of the European Union (21 June 2022)

Maximillian Schrems v Data Protection Commissioner (C-362/14), Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2015)

NG v Direktor na Glavna direktsia 'Natsionalna politsia' pri Ministerstvo na vatreshnite raboti – Sofia (C-118/22), Judgment, Grand Chamber, Court of Justice of the European Union (30 January 2024)

Patrick Breyer v Bundesrepublik Deutschland (C-582/14), Judgment, Court of Justice of the European Union (19 October 2016)

Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service (C-623/17), Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2020)

Spetsializirana prokuratura (C-350/21), Judgment, Court of Justice of the European Union (17 November 2022) (translated from the original French)

Tele2 Sverige AB v Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v Tom Watson et. al. (C-698/16), Joined Cases, Judgment, Grand Chamber, Court

V.S. v Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost, (C-205/21), Judgment, Court of Justice of the European Union (26 January 2023)

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).