NATIONAL DATA RETENTION LAWS: Privacy International's briefing on recent developments in the indiscriminate retention of communications data

December 2023

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 2.0 UK: England & Wales. 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.

Photo by Fred Moon on Unsplash

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

ACKNOWLEDGMENTS

This report has been compiled by Privacy International with the assistance of Gaëtan Goldberg. Special thanks to our partner organisations who provided their input in relation to national legal frameworks: ALT Advisory (South Africa), Asociación por los Derechos Civiles (ADC) (Argentina), Homo Digitalis (Greece), Internetlab (Brazil), and SMEX (Lebanon).

SUMMARY

Over the past years, data retention regulation imposing generalised and indiscriminate data retention obligations to telecommunication companies and Internet service provides has been introduced in various jurisdictions across the world. As the data retention practices across the world have evolved this new report is an attempt to shed some light on the current state of affairs in data retention regulation across ten key jurisdictions. Privacy International has consulted with human rights organisations to survey the legal systems of Argentina, Belgium, Brazil, France, Germany, Greece, Lebanon, Mexico, Tunisia, and South Africa. This report highlights that while the regulation within the EU continues to present challenges, regulatory frameworks across three different continents present similar concerns by introducing vague regulatory frameworks, lacking procedural safeguards and human rights protection exposing the communications and personal data of millions of users of telecommunications networks to unlawful access and abuse.

ABBREVIATIONS

ADAE	Hellenic Authority for Communication Security and Privacy (Greece)
ANATEL	Telecommunication Regulatory Agency (Brazil)
App No	Application Number
CJEU	Court of Justice of the European Union
CNCTR	Commission responsible for monitoring intelligence techniques (France)
DPA	Data Protection Authority
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
FIT	Federal Institute of Telecommunications (Mexico)
FTB	Federal Telecommunications and Broadcasting Law (Mexico)
GC	Grand Chamber
HDPA	Hellenic Data Protection Authority (Greece)
ibid	*ibīdem*, meaning "in the same place"
ICCPR	International Covenant on Civil and Political Rights
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ISPs	Internet service providers
LGPD	General Personal Data Protection Law (Brazil)
N/A	Not applicable
OHCHR	Office of the United Nations High Commissioner for Human Rights
PANAUT	National Registry of Mobile Telephony Users (Mexico)
PEI	Permanent equipment identifier
RICA	South Africa's Regulation of Interception of Communications and Provision of Communication-related Information Act (South Africa)
s./ss.	section/sections
SUCI	Subscription Concealed Identifier (Belgium)
SUPI	Subscription Permanent Identifier (Belgium)
TKG	German Telecommunications Act
UN	United Nations
UNGA	UN General Assembly

INTRODUCTION

The practice of mandating by law the retention of communications data (or metadata) by private companies raises significant privacy, transparency, and security concerns. Yet states across the world continue to require telecommunications companies and Internet service providers by law to store large amounts of personal data on an ongoing basis for later access by state agencies, including intelligence agencies, law enforcement and local authorities. We are concerned because such storage and access are often indiscriminate and fails to guarantee sufficient safeguards from abuse. Also, as the amount of data generated by smartphones and other connected devices increases, the data mandated for retention becomes an exponentially increasing pool of ever more personal and sensitive data for disposal by the state authorities.

Multiple human rights monitoring bodies and independent experts – including the UN Human Rights Committee, Special Rapporteur on freedom of opinion and expression, and others – have highlighted the risks that mandatory data retention and have found current practices to be inconsistent with human rights standards.[1] The UN High Commissioner for Human Rights has more recently observed:

> *[…] 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. […]*[2]

1 Indicatively, Concluding Observations on the Eighth Periodic Report of Ukraine, UN Doc CCPR/C/UKR/CO/8 (11 November 2021); 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). See also below section on "Data Retention under International Human Rights Law".

2 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) para 18 (emphasis added) (hereinafter OHCHR, A/HRC/39/29 (2018)).

In the EU, the Court of Justice of the European Union (CJEU) has repeatedly reaffirmed that all data retention regimes must comply with the principles of legality, necessity, and proportionality.[3] Despite multiple judgments by the CJEU over the years, several EU member states' data retention regimes continue to lack clarity and have been the subject of prolonged challenges before national courts. While the Court was clear in stating that the collection of data by national authorities must comply with privacy safeguards as set under EU law, member states are still trying to deploy creative workarounds requiring general and indiscriminate retention of communications data.[4] Outside the EU, data retention practices have been also expanding where not only telecommunications companies indiscriminately retain data for future law enforcement purposes, but also other companies, such as in Tunisia where internet services providers are also required to retain communications data for a minimum period of two years.[5] In Brazil, the law has expanded its reach to apply also to online platforms.[6]

3 CJEU, *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH* (Joined Cases C-793/19 and C-794/19), Judgment, 20 September 2022 (hereinafter CJEU, *SpaceNet/Telekom Deutschland* cases); CJEU, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (C-623/17), Judgment, 6 October 2020 (hereinafter CJEU, *Privacy International* case); *La Quadrature du Net and others v Premier Ministre and others* (Joined Cases C-511/18, C-512/18 and C-520/18), 6 October 2020 (hereinafter CJEU, *La Quadrature du Net and others* cases); CJEU, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* (Joined cases C-203/15 and C-689/15), Judgment, 21 December 2016 (hereinafter CJEU, *Tele2/Watson* cases (2026)).

4 Similar issues have been identified at the EU level where the European Data Protection Supervisor (EDPS) had to request that the CJEU annuls two provisions of a newly amended Europol Regulation that would have the effect of retroactively legalising the European Union Agency for Law Enforcement Cooperation (Europol)'s processing of large volumes of individuals' personal data with no established link to criminal activity. See EDPS, Press release, EDPS/2022/23, (22 September 2022) https://edps.europa.eu/system/files/2022-09/EDPS-2022-23-EDPS-request%20to%20annul%20two%20new%20Europol%20provisions_EN.pdf

5 See section below 'Tunisia'.

6 See section below 'Brazil'.

RECOMMENDATIONS

Considering the concerns raised in this report, Privacy International recommends:

To all states to review their legislation with the view to:

- prohibit the imposition of a requirement of general and indiscriminate retention of communications data in all circumstances;
- refrain from imposing data retention obligations, and in any case ensure that any obligation complies with the principles of legality, necessity and proportionality;
- subject any imposition of data retention and access to retained data to prior judicial authorisation; and require that such retention is limited only to the data and time that is strictly necessary for the prevention or investigation of serious crimes or serious national security threat;
- provide for independent oversight mechanism and for notification of the persons affected in order to ensure the right to effective remedy.

To telecommunications and internet service providers and other companies subjected to data retention obligations to:

- support legislative reforms to bring data retention legislation in line with international human rights law;
- challenge data retention and data access requests by state authorities that do not meet the requirements of legality, necessity and proportionality;
- publish requests by State authorities to retain and access data;
- inform users in a clear, easily accessible and age-appropriate way about the collection, use, sharing and retention of their data;
- adopt privacy and data protection policies in accordance with international data protection standards.

METHODOLOGY

In 2017, Privacy International published a report that examined the developments in data retention regulation across the EU post the *Tele-2/Watson* judgment by the Court of Justice of the European Union.[7] Since then, data retention regulation has been introduced in various jurisdictions across the world, while the regulation within the EU continues to present challenges.

As the data retention practices across the world have evolved this new report is an attempt to shed some light on the current state of affairs in data retention regulation across ten key jurisdictions. Privacy International has consulted with human rights organisations to survey the legal systems of Argentina, Belgium, Brazil, France, Germany, Greece, Lebanon, Mexico, Tunisia, and South Africa. These countries have mandatory data retention legislation (explicitly or de facto); their political system is democratic (or at least in transition to democracy); and spread across different continents (Africa, America, and Eurasia). All countries are party to the International Covenant on Civil and Political Rights and Argentina, Belgium, France, Germany, Greece, Mexico, and Tunisia are all parties to Council of Europe Convention 108.[8]

Tracking legislation and jurisprudence across different jurisdictions is often a challenge: while this report aims to provide accurate and complete information on the national data retention regimes covered therein to date, Privacy International would be grateful to receive any additional information, updates and clarification. Please reach out at research [@] privacyinternational.org

---

7 PI, 'A Concerning State of Play for the Right to Privacy in Europe National Data Retention Laws since the CJEU's Tele-2/Watson Judgment' (2017), https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf

8 Chart of signatures and ratifications of Treaty 108, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108

OVERVIEW OF DATA RETENTION PRACTICES: SETTING THE SCENE

WHAT DATA

The practice of data retention involves the gathering and storing of communications data, also known as "metadata", for extended periods for the purpose of future access and analysis. Communications data provides the who, when, what, and how of a specific communication – as opposed to "content data" which contains the actual content of a communication.[9]

Data collected will likely cover a mixture of personally identifiable and non-identifiable information, including:

- traffic data (data about how a communication was transmitted including source, destination, means of transmission, time and location of transmission);
- subscriber data (data identifying subscribers as provided to the communications service provider); and
- data specific to the use of the communications service in question (time of use, billing information, amount of data downloaded, redirection services).[10]

9 PI, 'How intrusive is communications data?' (21 August 2019) **https://privacyinternational.org/long-read/3176/how-intrusive-communications-data**

10 *ibid.* See also David Anderson, A Question of Trust: Report of the Investigatory Powers Review (June 2015) para 6.6 https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf

As the UN General Assembly reiterated that

> 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.[11]

WHAT RETENTION COVERS

Data retention in general terms describes the practice of storing and managing data and records for usually a designated period. Data retention allows for future access, transfer, analysis of this data for a variety of purposes. Data retention broadly serves multiple uses, some of which are commercial (e.g. necessary for provision of service by communication providers) and others not.

Data retention can be voluntary, for instance where the data is kept by a company for its internal uses (e.g. to better understand their customers' use of the service) or it can be mandated by law for potential access by third parties, in particular by state agencies for law enforcement and intelligence purposes. As such the legal framework regulating data retention and as a result its legal basis may differ. **This briefing examines the current legal frameworks in 10 jurisdictions regulating mandatory retention of communications data that are imposed by state authorities to telecommunications and internet service providers.** There is an increasing tendency to impose such obligations to social media companies and other communications service providers. However, these are not covered here.

---

11 UNGA Resolution on the right to privacy in the digital age, UNGA Res 77/211, preambular para 20. Also, the UN Special Rapporteur on the right to privacy highlighted that "techniques such as the collection and analysis of metadata referring to protocols of internet browsing history, or data originating from the use of smartphones (location, telephone calls, use of applications, etc.) are subject to much weaker safeguards. That is not justified, since the latter categories of data are at least as revealing of a person's individual activity as the actual content of a conversation. Hence, appropriate safeguards must also be in place for these measures." Report of the Special Rapporteur on the right to privacy, UN doc A/HRC/34/60 (6 September 2017). Similarly, CJEU said metadata "is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained". CJEU, *Digital Rights Ireland Ltd v Minister of Communications, Marine and Natural Resources and others* (C-293/12), 8 April 2014, para 27 (hereinafter CJEU, *Digital Rights Ireland* case (2014)); CJEU, *Tele2/Watson* (2016), note 3, para 99.

HARMS AND RISKS

In a context where data volumes have been growing exponentially and the gathering, storage, and exploitation of data, facilitated by artificial intelligence and machine learning, by private companies and state agencies becomes increasingly intrusive, data retention poses serious risks to individual privacy and data security.[12] Retained communications data enables state authorities and third parties to make intimate inferences about individuals, to engage in profiling, and to otherwise intrude on people's private lives.[13] These threats should be further evaluated in light of the role of the right to privacy as an enabler for the enjoyment of other rights. Any interference with privacy often provides the gateway to the violation of other human rights.[14] For example, the intrusive nature of data retention practices can induce chilling effects on the right to freedom of expression, which was recognised by courts and human rights bodies.[15]

Privacy has become even more essential in the age of data exploitation. Data retention puts vast amounts of personal data at risk of abuse by state authorities and others. If the information is not properly protected, there is potential for unauthorised access to troves of information by third parties, including criminals. Communications data can have an important role to play in criminal investigations, yet the retention of such data should not violate applicable human rights standards.[16]

---

12 Recognised among others by the UN High Commissioner for Human Rights in their 2018 report on the right to privacy in the digital age. OHCHR, A/HRC/39/29 (2018), note 2, para 18.

13 As noted by the CJEU in the *Tele2/Watson* decision, retained data allows for the drawing of "very precise conclusions… concerning the private lives of the persons whose data has been retained… In particular, that data provides the means… of establishing a profile of the individuals concerned" (see note 3, para 99).

14 PI, "Privacy Matters", https://privacyinternational.org/learning-resources/privacy-matters

15 CJEU, *Digital Rights Ireland* case (2014), note 11, para 28; CJEU, *Tele2/Watson* (2016), note 3, para 101.

16 For example, the next generation of telecommunications systems, 5G, will be able to pinpoint location data with much more precision than previous systems, aggravating privacy risks of location data retention. PI, 'Welcome to 5G: Privacy and Security in a Hyperconnected World (Or Not?)' (23 July 2019) https://privacyinternational.org/long-read/3100/welcome-5g-privacy-and-security-hyperconnected-world-or-not

DATA RETENTION LEGAL FRAMEWORKS

As already mentioned, this briefing focuses on data retention frameworks and not the regime regulating the access and analysis of data. Laws in most countries treat separately the retention of data and the access to it for law enforcement or intelligence purposes. The two issues are, however, closely intertwined.[17] Poorly drafted data retention legislation increases the chances of indiscriminate transfer, collection, and access of such data that increase the risk of abuses of data. For example, the absence of limitations on retention (e.g. the absence of proper deletion processes for irrelevant information or of proportionate retention periods) increases the likelihood of unauthorised access and security breaches. Similarly, broad, vague or ill-defined rules on governmental access to retained data can lead to unlawful surveillance, a rise in collateral data (that is, the incidental access to information of individuals who are not related to the subject of the investigation), misuse and other abuses of data protection standards (e.g. sharing of personal data).

Consequently, safeguards must be put in place to ensure that the interference with fundamental rights is minimised at both the retention and the access stages. There are already human rights standards on data retention developed by the UN human rights mechanisms, the European Court of Human Rights (ECtHR), the Council of Europe through Convention 108+ and the CJEU that seek to ensure that the individuals whose data is being retained are adequately empowered to protect themselves against all of these associated risks.[18] However, current national frameworks often do not seem to comply with those standards.

---

17 Melinda Rucz and Sam Kloosterboer, 'Data retention revisited, European Digital Rights', EDRi (2020), https://edri.org/wp-content/uploads/2020/09/Data_Retention_Revisited_Booklet.pdf, p 6 (hereinafter EDRi, 'Data retention revisited…').

18 'PI's Guide to International Law and Surveillance' (December 2021) https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance

There are serious questions raised in relation to the necessity of mandatory data retention practices, such as the existence of less intrusive alternatives and the fact that companies already keep what is necessary for business purposes. This briefing examines and analyses the shortcomings of existing legislative frameworks rather than the need for their existence. For an overview of key arguments and concerns see EDRi's Booklet on data retention.[19]

In the following pages we provide a brief overview of existing international human rights law standards, with a special mention to the EU jurisprudence. Subsequently, the national frameworks regulating mandatory data retention are presented.

19 EDRi, 'Data retention revisited…', note 17.

DATA RETENTION UNDER INTERNATIONAL HUMAN RIGHTS LAW

Any data retention practice needs to comply with international human rights standards on the right to privacy, as protected by international and regional human rights treaties.[20] When called to asses data retention practices, human rights courts and bodies have confirmed that data retention, whether indiscriminate or targeted, constitutes **an interference with the right to privacy**.[21] The UN Human Rights Committee, monitoring body of the International Covenant on Civil and Political Rights (ICCPR), has asserted that as a general rule countries should "refrain from imposing mandatory retention of data by third parties".[22] The UN High Commissioner for Human Rights recommended that states "review laws to ensure that they do not impose requirements of blanket, indiscriminate retention of communications data on telecommunications and other companies"[23] and the UN Human Rights Council in its 2023 resolution on the right to privacy in the digital age call on calls again on states "To refrain from requiring business enterprises to take steps that interfere with the right to privacy in an arbitrary or unlawful way".[24]

Human rights bodies have condemned **indiscriminate and generalised mandatory data retention as not permissible under international human rights** as it can never

20 Article 17, International Covenant on Civil and Political Rights (16 December 1966); Article 11, American Convention on Human Rights (Pact of San Jose), (22 November 1969); Article 8, European Convention for the Protection of Human Rights and Fundamental Freedoms (4 November 1950); Articles 7-8, Charter of Fundamental Rights of the European Union (2012/C 326/02) and others.

21 ECtHR, *S and Marper v The United Kingdom*, App Nos 30562/04 and 30566/04, Judgment (4 December 2008); CJEU, Digital Rights Ireland case, note 11; CJEU, *Kärntner Landesregierung and others* (Joined cases C-594/12 and others), Judgment, 8 April 2014, para 34; OHCHR, A/HRC/39/29 (2018), note 2.

22 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.

23 OHCHR, A/HRC/39/29 (2018), note 2, para 61(g).

24 UN Human Rights Council Resolution on the right to privacy in the digital age, UN Doc A/HRC/RES/54/21 (16 October 2023) para 10(p); UN Human Rights Council Resolution on the right to privacy in the digital age, UN Doc A/HRC/RES/48/4 (7 October 2021) para 6(n).

meet the standards required by the principles of necessity and proportionality.[25] They have particularly raised the alarm that broad mandatory data retention policies limit an individual's ability to communicate anonymously.[26]

In its concluding observations, the UN Human Rights Committee has elaborated on the safeguards required to ensure compliance with the ICCPR. The Committee has repeatedly noted that member states should bring its regulations governing data retention:

> *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.*[27]

The mandatory data retention practices should be also evaluated in light of standards developed by the European Court of Human Rights (ECtHR) in its jurisprudence relating to data retention more broadly (meaning beyond the limited focus of this briefing that analyses mandatory data retention imposed to

---

25 Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, UN Doc A/HRC/48/31 (13 September 2021) para 39; OHCHR, A/HRC/39/29 (2018), note 2, paras 17-18; 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) para 55. See also Box on below on 'Data Retention in the European Union' in relation to CJEU jurisprudence.

26 *ibid.*

27 Concluding Observations on the Eighth Periodic Report of Ukraine, UN Doc CCPR/C/UKR/CO/8 (11 November 2021) para 42. See also Concluding Observations on the Fourth Periodic Report of Paraguay, Human Rights Committee, UN Doc CCPR/C/PRY/CO/4 (20 August 2019) para 30; Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, UN Doc CCPR/C/ITA/CO/6 (28 March 2017) para 35-36; Concluding Observations on the Sixth Periodic Report of Italy, UN Human Rights Committee, UN Doc CCPR/C/ITA/CO/6 (28 March 2017) para 37; Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, UN Doc CCPR/C/GBR/CO/7 (17 August 2015) para 24; Concluding Observations on the Initial Report of South Africa, Human Rights Committee, UN Doc CCPR/C/ZAF/CO/1 (27 April 2016) paras 42-43.

telecommunications and internet service providers).[28] Among others, the ECtHR has consistently held that data retention constitutes an interference with Article 8 of the European Convention on Human Rights regardless of whether it is accessed later.[29] When it comes to appropriate safeguards, the European Court has for instance reiterated that personal data should be deleted as soon as they were no longer needed to achieve their statutory purpose.[30]

Data Retention in the European Union

When examining international human rights law standards on data retention, a special mention should be reserved to the jurisprudence of the Court of Justice of the European Union, jurisprudence stemming from cases brought at national level mostly as a result of civil society initiatives. At EU level, data retention obligations imposed on telecommunications providers originally derived from the Data Retention Directive (2006/24/EU),[31] which was annulled by the CJEU in the Digital Rights Ireland case in 2014.[32] In this landmark judgment, the Court held the Directive to be invalid.

Following the Digital Rights Ireland judgment, all national implementing measures transposing Directive 2006/24 into national law became incompatible with EU law. Member states were therefore required to repeal and amend their laws. However, in the absence of European

28 See analysis by Franziska Boehm and Mark Cole, "Data Retention after the Judgement of the Court of Justice of the European Union" (2014) https://www.zar.kit.edu/DATA/veroeffentlichungen/237_237_Boehm_Cole-Data_Retention_Study-June_2014_1a1c2f6_9906a8c.pdf, pp 21-27.

29 ECtHR, *S and Marper v UK*, note 21. See also ECtHR, *Roman Zakharov v Russia* [GC], App No 47143/06, Judgment (4 December 2015); ECtHR, *Gaughran v The United Kingdom*, App no 45245/15, Judgment (13 February 2020).

30 ECtHR, *Weber and Saravia v Germany*, App No 54934/00, Decision (29 June 2006) para 132.

31 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105, 13.4.2006, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0024

32 CJEU, *Digital Rights Ireland* case (2014), note 11.

legislation, several member states continued to apply their national legislation on data retention. This led to new cases reaching the Court.

Examining these data retention regimes, the Court further clarified the conditions that national data retention legislation must meet in order to be lawful. In *Tele2/Watson* (2016), the CJEU asserted minimum safeguards of EU law that must be prescribed in any national data retention legislation. In short, the Court affirmed that there needs to be legislation providing, as a preventive measure, for

the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.

It highlighted the need for clear and precise rules regarding the scope and application of data retention and imposing minimum safeguards. Data retention should be limited to what is strictly necessary to the objective pursued.[33]

In this case, the Court made clear that member states may not mandate the general and indiscriminate retention of all traffic and location data for the purpose of fighting crime. Yet this approach did not convince a number of member states, which considered the retention of communications data for the purpose of safeguarding national security to fall outside the scope of EU law. This objective had not been clearly defined and more cases reached the CJEU.

33 CJEU, *Tele-2/Watson* cases (2014), note 3, paras 108-111.

In three recent judgments, the Court successively considered data retention schemes in the UK, France, Belgium, and Germany. In Privacy International, the Court ruled that EU law applies every time a national government forces telecommunications providers to process data, including when it is for the purposes of national security. In the joint cases of La Quadrature du Net and Others v France and Ordre des barreaux francophones and germanophone and Others v Belgium, the Court defined the applicable limits to the use of the national security[34] exception to the protection of fundamental rights enshrined in the EU Charter. It did not rule out the automated analysis of traffic and location data for national security purposes, finding the practice to be justifiable should it meet the strict necessity test.[35] In SpaceNet AG and Others, the Court considered that EU law precludes the general and indiscriminate retention of traffic and location data, except in the case of a serious threat to national security where member states may, in strict compliance with the principle of proportionality, provide for the targeted or expedited retention of such data and the general and indiscriminate retention of IP addresses.[36]

34 CJEU, *Privacy International* case (2020), note 3; See also Privacy International, 'CJEU Bulk Challenge' https://privacyinternational.org/legal-action/cjeu-bulk-challenge

35 CJEU, *La Quadrature du Net and others cases* (2020), note 3, para 176.

36 CJEU, *SpaceNet/Telekom Deutschland* cases, note 3.

DATA RETENTION LAWS IN 2023: THE CURRENT STATE OF AFFAIRS

State authorities across the world have been slow to review and adapt their data retention legislation in line with applicable international human rights standards.

The CJEU judgments have forced EU member states to review their data retention laws with a view to reducing retention periods, and subjecting retention obligations and access rights to stricter conditions and safeguards. While EU states have an obligation to ensure that their laws comply with the CJEU's jurisprudence, it is concerning to note that only a limited number of member states have actually amended their legislation to comply with CJEU judgments. Some of the revised laws are still being drafted, while some are already subject to new legal challenges, as governments keep attempting to impose the widest possible retention requirements on telecommunications and internet service providers. Of the EU countries examined in this briefing, only Belgium seems to have designed more targeted retention requirements albeit with broad exceptions covering large geographical areas, while other EU member states are still expressly mandating bulk data retention in their legislation. Germany had introduced shorter retention periods of time but yet still imposed indiscriminate and generalised retention periods.

Outside the EU, the number of data protection laws are growing, as is the number of data retention laws. Mandatory retention periods in the countries examined range from 6 months to 7 years. However, many states continue to rely on outdated, vague intelligence/surveillance laws to impose data retention requirements and fail to review their laws to comply with existing human rights and data protection standards. Very few governments have taken the lead in pushing legal reforms, and to the extent that limited positive changes at the national level have occurred, they have been the result of constitutional challenges that have forced the establishment of stricter safeguards around access to retained data (such as in South Africa or Brazil), but bulk data retention requirements remained untouched.

In the next section we provide an overview of the data retention and access frameworks of ten countries, with a summary of legal developments that led to the current state of affairs.

COUNTRY OVERVIEWS

ARGENTINA

There is no specific legislation requiring traffic data retention in Argentina. The country issued a data retention law for traffic data in 2004,[37] compelling telecommunications services and Internet service providers to retain data for 10 years. However, in the 2009 *Halabi case the Supreme Court invalidated the law on the basis that it constituted a "drastic interference" with the right to privacy.*[38] Nonetheless, Law 25.891 on Mobile Communications Services requires the maintenance of a National Public Registry of Mobile Network Users where mobile telecommunications companies must register all users' personal data.

Some provisions regarding accessing these records are set in criminal law. The Criminal Procedure Code establishes that a judge can grant access to any records of an accused's communications or those who communicate with them. Public prosecutors can also request direct access to these records in an emergency, and only in some specific crimes that the Criminal Code has previously established. However, in these cases, it must immediately notify a judge, who has 24 hours to validate the request.[39]

37 Telecommunications Law 25.873 (6 February 2004) http://servicios.infoleg.gob.ar/infolegInternet/anexos/90000-94999/92549/norma.htm

38 Centro de Información Judicial, 'La Corte crea acción colectiva y da alcance general a un fallo' (24 February 2009) https://www.cij.gov.ar/nota-615-La-Corte-reconoce-accion-colectiva-y-da-alcance-general-a-un-fallo.html

39 Article 236, Argentine Criminal Procedure Code (21 August 1991) http://www.infoleg.gov.ar/infolegInternet/anexos/0-4999/383/texact.htm

LEGAL BASIS	PURPOSES	CATEGORIES OF DATA	RETENTION PERIOD	ACCESS
Law 25.891 on Mobile Communications Services[40]	Create the National Public Registry of Users and Clients of Mobile Network Communications Services	Data allowing clear identification of the account holders and the final users:* • Subscriber information (personal data) • Filial data[41] • Address details **If the account holder differs from the final users of the mobiles*	Indefinite	Public prosecutor office (only in the cases established by law 25.873) and Any state authority following judicial order

Commentary

In Argentina, there is no specific law imposing bulk data retention. However, Law 25.891 on Mobile Communications Services includes provisions that impose general data retention obligations. One of the most pressing concerns with Law 25.891 is the absence of specific requirements regarding data retention periods. Consequently, mobile companies are indirectly permitted to indefinitely retain personal data and sensitive information, including criminal records. This indefinite data retention raises significant privacy issues, potentially leading to misuse and unauthorized access to critical records and sensitive information.

Moreover, the law's language concerning the scope of data retention is notably ambiguous. While it outlines a minimum requirement for data retention (filial data or address information), it also states that mobile network companies should retain all information to identify account holders and users. This vagueness leaves room for misinterpretation and overreach by companies, potentially resulting in

40 Mobile Communications Services Law, Law 25.891 (28 April 2004) http://servicios.infoleg.gob.ar/infolegInternet/anexos/95000-99999/95221/norma.htm

41 Filial data according to Argentinian legislation (Law 952/2022) are data of members of family and could include information such as: last name, first name, ID number, date and place of birth; and, if applicable, date and place of death and parents. (26 August 2022) https://servicios.infoleg.gob.ar/infolegInternet/anexos/370000-374999/370678/norma.htm26

excessive data collection. On the other hand, Law 25.891 imposes disproportionate obligations on mobile companies by mandating their availability to national and provincial security forces. This includes offering a free call service at all hours and days of the year for verification purposes.

The Criminal Procedure Code establishes that a judge must issue a court order to access that data. However, it also states that if there are risks associated with delays, a public prosecutor can access the register directly. Supposedly, this is limited to specific crimes, but the article enumerates an extensive range of them, including crimes against liberty and property and those «in relation with the». This broad spectrum of offenses raises concerns about potential data misuse and expands the scope of access to law enforcement agencies without adequate safeguards. Clear safeguards and security protocols detailing how the retained data should be protected are absent from both laws containing these provisions. The laws mandate data retention but do not provide explicit guidance on necessary security measures, potentially exposing data to breaches and privacy violations.

BELGIUM

In Belgium, the 2021 CJEU judgment led to radical changes in the country's data retention framework.[42] Successively regulated by the law of 30 July 2013 and the law of 29 May 2016, the retention of traffic and location data was very much inspired by the 2006 Data Retention Directive, annulled in the *Digital Ireland* case.[43] On 22 April 2021, in a landmark judgment the Belgian Constitutional court ruled that the general and indiscriminate retention of traffic and location data for one year violates the right to privacy and the right to protection of personal data and annulled the relevant provisions of the law of 29 May 2016, enjoining the legislator to draw up a new regulation in light of the clarifications made by the CJEU in *La Quadrature du Net and others*.[44] The law of 20 July 2022 attempts to introduce a targeted mechanism that imposes obligations according to geographical criteria and the level of criminality in pre-determined areas.[45]

---

42 Law on the collection and retention of identification data and metadata in the electronic communications sector and the provision of such data to the authorities (original in French: Loi relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités), C-2022/15454 (20 Juillet 2022) http://www.ejustice.just.fgov.be/eli/loi/2022/07/20/2022015454/moniteur (hereinafter C-2022/15454).

43 CJEU, *Digital Rights Ireland* case (2014), note 11.

44 CJEU, *La Quadrature du Net and others* cases (2020), note 3, para 176.

45 C-2022/15454, note 41.

LEGAL BASIS	PURPOSES	CATEGORIES OF DATA
LAW OF 20 JULY 2022	To establish fraud or malicious use of the network or service or identify its author and origin Detecting or analysing fraud or malicious use of the network	Traffic data, including: • the identifier of the origin of the communication • the identifier of the destination of the communication • the precise dates and times of the commencement and termination of the call • the location of the terminal equipment of the parties to the call at the beginning and end of the call.
		Traffic data used to identify the originator of the communication: • telephone number from which the incoming communication originated, or • IP address used to send the incoming communication, time stamp and port used • the precise dates and times of the start and end of the incoming communication • Location data
	Safeguarding national security, combating serious crime, preventing serious threats to public security, and safeguarding the vital interests of a natural person	• National Register number or equivalent, name and surname of the end-user for natural persons or name of the subscriber for legal entities • The alias, if any, chosen by the end-user when subscribing to the service • Subscriber's contact details • Date and time of the subscription to the service and of the activation of the service and the elements allowing to determine the place from which this subscription and activation were made • Physical delivery address of the service • Billing address of the service and data relating to chosen method of payment, date of payments, transaction reference in case of online payment • The main service and the ancillary services that the subscriber may use; • The date from which services can be used, date of the first use and date of termination • In case of transfer of the subscriber's identifier, the identity of the operator transferring the identifier and the identity of the operator to whom the identifier is transferred, the date on which the transfer is made • The assigned telephone number • The main email address and email addresses used as aliases • International Mobile Subscriber Identity (IMSI) • Subscription Permanent Identifier (SUPI) • Subscription Concealed Identifier (SUCI)

	RETENTION PERIOD	ACCESS
	4 months from the date of the communication; if a specific fraud or a specific malicious use of the network is identified, the time needed for analysis and resolution can go beyond 4 months	Persons responsible for: • billing • traffic management • handling subscriber enquiries • combating fraud or misuse of the network • network security • compliance teams In the event of suspected fraud or misuse operators may transmit to the competent authorities all data lawfully held in relation to the data legally retained in connection with the suspected fraud or misuse.
	12 months from the date of the communication; if a specific malicious use is identified, the time needed for analysis and resolution can go beyond 4 months from the date of the communication, except in cases of fraud or specific malicious uses which require the data concerned to be retained beyond that period	
	As long as the electronic communications service is used and 12 months after the end of the service	

LEGAL BASIS	PURPOSES	CATEGORIES OF DATA
LAW OF 20 JULY 2022		• The IP address at the source of the connection, the time stamp of allocation and, in the case of shared use of an end-user IP address, the ports that have been assigned to them • The end-user device identifier, or where the operator does not process or generate it, the identifier of the equipment that is closest to that terminal equipment, namely IMEI, PEI, MAC address
	Safeguarding national security, combating serious crime, preventing serious threats to public security, and safeguarding the vital interests of a natural person in specific geographical areas set on a yearly basis: • Judicial districts with high crime rates • Areas where there is a potential serious threat to the vital interests of the country or to the basic needs of the population	• All of the above • Electronic communications metadata, including metadata for unsuccessful calls: ◦ Date and exact time of the start and end of the session ◦ Data enabling the identification and location of cells or other termination points in the mobile network which were used to make the call; ◦ Volume of data sent to the network and downloaded during the session ◦ Date and time of connection of the device to the network, date and time of disconnection ◦ Location of the device + date and time of that location whenever the operator seeks to know which device is connected to its network

	RETENTION PERIOD	ACCESS
	12 months after the end of the session 6 months when the provider retains the IMEI, PEI or MAC address	Intelligence services Competent authorities for the purpose of preventing serious threats to public security Authorities responsible for safeguarding the vital interests of natural persons Administrative or judicial authorities responsible for the prevention, investigation, detection or prosecution of an offence committed via an electronic communication network or service Administrative or judicial authorities competent for the prevention, investigation, detection or prosecution of serious crimes Other relevant authorities as prescribed by law
	12 months from the date of the communication, except if another duration is set by law In judicial districts targeted for their high crime rates, durations vary between 6, 9 and 12 months depending on crime rates When the communication takes place in part inside one of the specific geographical areas and outside, the shorter storage limitation applies	

Commentary

The new Belgian data retention regime no longer contains a general data retention obligation. The principle now is that telecommunications providers must delete traffic and location data or make such data anonymous as soon as it is no longer necessary for the transmission of the communication. However as detailed above an important number of exceptions provide for circumstances in which significant amounts of metadata may still be retained in targeted geographical areas. The list of circumstances justifying such exceptions includes in order to safeguard national security or vital interests, to combat serious crime and to prevent serious threats to public security. They can all be broadly interpreted. For instance, the calculation of the high crime rates includes ordinary offences such as forgery, fraud, or drug possession. Also, the list of specific geographical areas covers vast portions of the Belgian territory. A member of the European Parliament estimated that almost the whole country could be considered a high crime rate area under the current classification[46] – in fact, this is a situation the law accounts for in case of a national threat.

Oversight of the processing of the data retained is divided among the national data protection authority, the Belgian Standing Intelligence Agencies Review Committee (the Standing Committee),[47] and the Supervisory Body for Police Information Management, depending on the services or party that access the retained data. It is notable and welcomed that a dedicated oversight body, the Standing Committee, monitors compliance of the Belgian intelligence services, as intelligence agencies often escape effective oversight. Yet, data subjects seem not to be notified that their data has been retained in most cases, hence are not aware they can challenge this retention. Also, acting on a complaint the Standing Committee may, for example, decide that the service concerned must correct or delete certain personal data. However, the Committee is not allowed to state whether or not the service in question stored personal data about the applicant

46 See Patrick Breyer, "'Targeted' Data retention: online map shows what the Belgian government wants to hide", (7 June 2022) https://www.patrick-breyer.de/en/targeted-data-retention-online-map-shows-what-the-belgian-government-wants-to-hide/

47 See Belgian Standing Intelligence Agencies Review Committee, Complaints and denunciations, https://www.comiteri.be/index.php/en/complaints-and-denunciations/complaints-and-denunciations-2#can

and there is no possibility to appeal its decisions. Only when data subjects can demonstrate a personal and legitimate interest can the Committee act as a judicial body and perform a control of the legality of the specific methods involved. If the Standing Committee notes that the decisions regarding specific methods are illegal, it can order the termination of the method and prohibit the exploitation of the data collected using this method and order their erasure.

BRAZIL

Brazil has several different general and sectoral laws that mandate data retention that establish in fact indiscriminate and generalised data retention obligations even if not explicitly recognising it. Most notably, the Marco Civil da Internet (*Brazilian Civil Rights Framework for the Internet*) requires ISPs to retain connection records for a year. Authorities then have relatively generous rights to access retained data, in some circumstances without the need for a court order. Also, the telecommunication regulatory agency (ANATEL) issued resolution 738/2020, which requires telephone traffic and internet connection records to be retained by providers to ensure permanent monitoring of legal and regulatory obligations.

Previously, the Brazilian telecommunications regulatory authority, enforced resolutions 426/05 and 477/07, imposing broad obligatory data retention requirements. Mobile telephone records and personal data had to be retained for a minimum of five years under these regulations, accessible to ANATEL and other interested parties. However, a more recent resolution, 738/2020, has revoked these regulations and appears to impose stricter conditions.

LEGAL BASIS	PURPOSES	CATEGORIES OF DATA
Marco Civil da Internet, Art 13[48]	N/A	• Connection records: subscriber data, • traffic data • duration, • connection logs • IP addresses
Marco Civil da Internet, Art 15	N/A	Records of access to Internet applications (by Internet application providers)
Resolução nº 738/2020, Art. 65-J, I (Telecommunication providers)	Ensure permanent inspection and monitoring of legal and regulatory obligations	tax documents subscriber registration data ticketing data calls made and received date, time, duration and value of the call
Resolução nº 738/2020, Art. 65-J, I (Telecommunication providers)	Ensure permanent inspection and monitoring of legal and regulatory obligations	Internet Connection records: • Date and time of the start and end of an Internet connection • Duration • IP address used by the terminal • Logical ports used when sharing a public IP, for sending and receiving data packets
Federal Law No. 12/850/13, Art 17[49]	Criminal investigations	Records identifying the numbers of the terminals where international, long-distance and local telephone calls originate and end

48 *Brazilian Civil Rights Framework for the Internet (original in Portuguese:* Marco Civil da Internet), Law No 12.965 (23 April 2014) https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180

49 Federal Law No 12.850 (2 August 2013) http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm

	RETENTION PERIOD	ACCESS
	1 year	Police, intelligence agencies, government agencies, local authorities, judiciary (requires a court order, except for subscriber data)
	6 months	Police, administrative authorities, Public Prosecutor's Office, judiciary (requires a court order)
	For a minimum period of 5 years	Brazilian telecommunications regulatory authority (Anatel)
	For a minimum of 1 year	Brazilian telecommunications regulatory authority (Anatel)
	5 years	Chief of Police and Public Ministry (without need for a court order)

Commentary

The *Brazilian Civil Rights Framework for the Internet* (Marco Civil da Internet) raises significant privacy concerns regarding data retention and authorities' access. According to this framework, ISPs are obligated to retain subscribers' records for one year. Compounding the privacy implications, authorities have relatively broad access rights to this retained data, sometimes without the need for a court order. Additionally, Article 13(3) of the *Brazilian Civil Rights Framework for the Internet,* allows administrative, police authorities, or the Public Prosecutor to request the precautionary extension of data retention beyond the one-year period specified in Article 13. However, a safeguard is articulated in Article 16, which prohibits the retention of access records to other Internet applications without users' explicit consent, as well as the retention of personal data beyond the originally consented purpose.

Brazil's General Personal Data Protection Law (LGPD)[50] requires data to be deleted as soon as the purpose for which it is was collected is realised. In a case challenging the retention of data by public entities for the purpose of fighting COVID-19 (ADI 6387), the Federal Supreme Court found that the retention of data for 30 days after the end of a public health emergency was excessive.[51]

According to the Brazilian telecommunications regulatory authority, ANATEL, service providers must maintain user data in a controlled and secure environment, deleting it promptly once its processing purpose is fulfilled or when legal or regulatory retention obligations expire, aligning with Brazil's General Personal Data Protection Law. Nevertheless, Article 65-J of Resolution 738/2020 stipulates that providers must retain specific data related to their services that allow telephone traffic to be carried for a minimum of five years and one year for services that allow Internet connection. These requirements raise concerns due to their extensive scope, even if applicable only to regulatory processes and accessible only to ANATEL. Furthermore, these regulations lack specifications regarding the maximum retention limit, posing a notable concern for potential indefinite data retention and associated vulnerabilities or security issues.

---

50 General Personal Data Protection Law, Law No 13.709 (14 August 2018) as amended by Law No 13.853 (8 July 2019), http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

51 Referendum on the precautionary measure in the direct action of unconstitutionality (original in Portugese: referendo na medida cautelar na ação direta de inconstitucionalidade) (07 May 2020) https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false

FRANCE

In France, intelligence and police services have long relied on data retention, including the indiscriminate retention of traffic and location data, which has been challenged in courts several times by human rights organisations.[52] Taking stock of previous CJEU judgments,[53] France had to make several adjustments to its data retention legislation. Following the 2021 decision by the Conseil d' État,[54] the Law 2021-998 of 30 July 2021 relating to the prevention of terrorist acts and intelligence was introduced.[55] Subsequently, the Prime Minister issued Decree 2021-1363 of 20 October 2021 mandating the 1-year retention of certain types of communications data. The decree refers to the "serious and present threat to [French] national security" to justify this blanket retention mandate.[56] No further justification was provided by the French government.

52 See for instance Louis Adam, 'Les exégètes amateurs écornent une nouvelle fois la loi Renseignement', ZDNET (21 October 2016) https://www.zdnet.fr/actualites/les-exegetes-amateurs-ecornent-une-nouvelle-fois-la-loi-renseignement-39843674.htm

53 CJEU, Privacy International case (2020), note 3. See also CJEU, *La Quadrature du Net and others* cases (2020), note 3.

54 The Conseil d' État found the generalised retention of traffic and location data for the purposes of prosecuting criminal offences and protecting the public order to be unlawful. However, the Court also found that the generalised retention of certain categories of data (civil status, IP address, accounts and payments data) was permissible. It also concluded that generalised retention of traffic and location data for national security purposes was lawful, provided that the government regularly assesses the existence of a grave, real, and actual or foreseeable threat to national security. See Conseil d' État, *French data network and others*, N° 393099 and others, AJDA 828 (21 April 2021) https://www.conseil-etat.fr/fr/arianeweb/CRP/conclusion/2021-04-21/393099?download_pdf

55 Law 2021-998 on the prevention of terrorist acts and intelligence (original in French : Loi n° 2021-998 relative à la prévention d›actes de terrorisme et au renseignement) (30 July 2021) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043876100

56 Decree 2021-1363 ordering the retention of certain categories of connection data for a period of one year in view of the current serious threat to national security (original in French: Décret n° 2021-1363 portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion) (20 October 2021) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044228976

LEGAL BASIS	PURPOSES	CATEGORIES OF DATA	RETENTION PERIOD	ACCESS
Law no 2021-998 of 30 July 2021 relating to the prevention of terrorist acts and to intelligence, Article 17	Criminal proceedings, the prevention of public security threats and the safeguarding of national security	Information relating to the identity of the user, including: • Surname and first name • Date and place of birth • for a legal entity: corporate name, surname, first name, date and place of birth of the person acting on its behalf • Postal address • Email address • Telephone number	5 years from the end of the contract	Public prosecutors, investigators or investigating judges (subject to reform, see section below)
		Other information provided by the user when subscribing to a contract or creating an account, as well as payment information: • The identifier used; • The pseudonym(s) used; • Data intended to enable the user to check or change his or her password, if necessary, by means of a two-factor identification system; • The method of payment used; • The payment reference; • The amount; • The data, time and place in case of a physical transaction.	1 year after the end of the validity of the contract or the closure of the account	
	Combating serious crime and criminal offences, preventing serious public safety threats and safeguarding national security	Technical data enabling the source of the connection to be identified or data relating to the device used: • The IP address assigned to the source of the connection and the associated port; • The user identification number; • The identification number of the device; • The telephone number at the origin of the communication.	1 year from the connection or use of the terminal equipment	
	Safeguarding national security when a serious, current or foreseeable threat to the latter is identified	Additional categories of traffic and location data as listed by decree by the Prime Minister: • The technical details as well as the date, time and duration of each communication; • Data on additional services requested or used and their providers; • Technical data allowing the identification of the recipient(s) of the communication; • For operations carried out using mobile phones, data identifying the location of the communication.	1 year	

Commentary

Overall, this new regime is broad and requires telecommunications providers to retain more data than they ever did. Ruling on the former data retention regime in France, the CJEU found the general and indiscriminate retention of traffic data for a year for the purpose of combating market abuse offences including insider dealing to be unlawful.[57] Given the scope and 'untargeted' nature of the new legislation, the regime under consideration continues to raise serious doubts as to its conformity with EU law.

Furthermore, while the French data retention framework provides for an independent administrative body to oversee the use of intelligence techniques, the opinions of the national commission responsible for monitoring intelligence techniques (*Commission nationale de contrôle des techniques de renseignement* (CNCTR)) are non-binding. There is also no obligation to notify those whose data has been accessed. Formally, any person wishing to know if they have been under surveillance can be heard by the CNCTR, which can make a recommendation to the Prime Minister that the implementation be stopped, and the information collected deleted. With the 2021 law, the CNCTR, as well as data subjects, may file an appeal with the Conseil d' État should the Prime Minister ignore its recommendation. It remains to be seen how this will be implemented. In its 2021 annual report, for the first time, the CNCTR included statistical data relating to each of the intelligence techniques that it has monitored.[58]

Additionally, the regime authorising access to retained data is still unclear. Under French criminal procedure, several entities can access traffic and location data retained by telecommunications providers: the public prosecutor, an investigator or the investigating judge. In *La Quadrature du Net and others,* the CJEU made clear that access to lawfully retained data had to be authorised by a court or an independent administrative body.[59] Following this judgment, French courts found in four recent cases that public prosecutors' access to such data was

57 CJEU, *VD and SR* (Joined cases C-339/20 and C-397/20), Judgment (20 September 2022).

58 National Commission for the Supervision of Intelligence Techniques (original in French: Commission nationale de contrôle des techniques de renseignement), 6th Annual report (2021) https://cms.cnctr.fr/uploads/RAPPORT_CNCTR_2021_interactif_30c40b93e6.pdf?updated_at=2023-06-12T08:25:32.231Z

59 CJEU, *La Quadrature du Net and others* cases (2020), note 3.

incompatible with EU law.[60] They found that the French public prosecutors who direct the investigation procedure and, where appropriate, prosecute cases, do not have a neutral stance as required by EU law, because they are involved in the investigation.[61]

GERMANY

Germany has also a long-standing practice in regulating data retention. However, none of the adopted national laws so far have been deemed as in accordance with international standards and at the moment of writing discussions for a new legislation are ongoing. German law that transposed Directive 2006/24 into national law was nullified by the Federal Constitutional Court in 2008 already. A new legal framework was eventually introduced in 2015, the German Telecommunications Act (*Telekommunikationsgesetz* or TKG). Section 113b of the Act provided for the retention of traffic and location data relating to customers' telecommunications. However, after a series of legal challenges, the German Federal Administrative Court (*Bundesverwaltungsgericht*) found that section 113b of the Act was unconstitutional as it violated the right to informational self-determination and the right to the privacy of telecommunications enshrined in national law.[62] The German data retention saga finally ended with the CJEU ruling that the German data retention rules were not compatible with EU law, reiterating that EU law precludes the general and indiscriminate retention of traffic and location data, except in the case of a serious threat to national security.[63]

---

60 See Cour de cassation, 'Criminal investigation: retention of and access to connection data', Appeals n° 21-83.710, 21-83.820, 21-84.096 and 20-86.652 (12 July 2022) https://www.courdecassation.fr/en/toutes-les-actualites/2022/07/12/criminal-investigation-retention-and-access-connection-data

61 *ibid.*

62 Article 10, Basic Law (Grundgesetz), BVerfG, Order of the First Senate, 1 BvR 1873/13 (27 May 2020) http://www.bverfg.de/e/rs20200527_1bvr187313en.html, paras 1-275. See on cases that preceded the 2020 judgment Verwaltungsgericht Köln, 9 L 1009/16 (25 January 2017) https://www.justiz.nrw.de/nrwe/ovgs/vg_koeln/j2017/9_L_1009_16_Beschluss_20170125.html. The Federal Administrative Court asked CJEU to clarify compatibility of the German regulation on data retention with EU law. Press release no 66/2019 (25 September 2019) https://www.bverwg.de/en/pm/2019/66

63 CJEU, *SpaceNet/Telekom Deutschland* cases, note 3.

Rather than providing a full analysis of the German data retention law that has been largely discarded and is probably in the process of being redrafted, the present analysis will focus on a few key provisions that although sometimes much stricter than the French or the Belgian current frameworks still did not pass the CJEU's compatibility test.

FORMER §113 TKG	CJEU ANALYSIS IN *SPACENET*[64]

Purposes:
• Providers must make location and traffic data available to the police and prosecution on request:
  ◦ To enable authorities to prosecute serious crimes
  ◦ To prevent concrete risks for the body, life or freedom of a person
	The general and indiscriminate retention of traffic and location data is only allowed for the purpose of safeguarding national security in situations where the Member State is confronted with a serious threat to national security. Such threat must genuine and present or foreseeable. The instruction to retain data must be subject to effective review and can be given only for a period of time that is strictly necessary.

No justification is needed for the retention (indiscriminate collection)	• EU law precludes national legislation which provides, on a preventative basis, for the purposes of combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of traffic and location data. • However, targeted retention of traffic and location data can lawfully take place under strict conditions for the purposes of safeguarding national security, combating serious crime and preventing serious threats to national security.

Providers of publicly available telecommunication services must store:
• Traffic data:
  ◦ Telephone number
  ◦ Date, time and information on the service used
  ◦ IP address, a unique identification of the access point, attributed user ID
  ◦ Date, time of the Internet usage
• Location data:
  ◦ Identifier of the network cell used for a particular communication
	The general and indiscriminate retention of:
	• IP addresses assigned to the source of an internet connection; and
	• data relating to the civil identity of users of electronic communications systems
	can take place for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security (the German Constitutional Court had a stricter view in its judgment of 27 May 2020).

64 As taken from CJEU, 'The Court of Justice confirms that EU law precludes the general and indiscriminate retention of traffic and location data, except in the case of a serious threat to national security', Press release No 156/22 (20 September 2022) https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220156en.pdf

<table>
<tr><th>FORMER §113 TKG</th><th>CJEU ANALYSIS IN SPACENET</th></tr>
<tr><td>Retention periods:
• Location data: 4 weeks
• All other types of data: 10 weeks</td><td>Expedited retention of traffic and location data for a specified period of time is allowed for the purposes of combating serious crime and safeguarding national security

Yet

Retaining all traffic and location data as listed under TKG 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".</td></tr>
<tr><td>Providers must delete data stored pursuant to the retention requirements without undue delay, but no later than one week, after the retention period expired</td><td rowspan="3">The retention of and access to data constitute separate interferences with the fundamental rights of the persons concerned, requiring a separate justification. National legislation as regards access to retained data cannot, by its very nature, be capable of either limiting or even remedying the serious interference with the rights of the persons concerned which results from the general retention of those data.</td></tr>
<tr><td>All retained data must be stored locally within Germany (data residency requirement)</td></tr>
<tr><td>Communication content is excluded from the retention and residency requirements.</td></tr>
</table>

Commentary

The law that was introduced on 18 December 2015 was quite similar to the 2008 regime that transposed Directive 2006/24 and was already nullified by the German courts. Section 113b of the Act made it mandatory for communications providers to retain traffic and location data relating to their customers' telecommunications. As the CJEU made clear, although storage limitation, access to data and residency requirements were duly regulated under the TKG, the retention of data alone still violated data subjects' fundamental rights. It is interesting to note that the retention periods foreseen under the TKG were much shorter than those currently applied in other countries, such as France and Belgium. However, this aspect did not convince the CJEU to decide otherwise. The mere fact that such retention was general and indiscriminate and took place for purposes other than safeguarding national security was enough for the Court to invalidate the framework as contrary to EU law. In this case, the Court has provided some guidance that could be followed by Germany, particularly in relation to the expedited retention of data that the Minister of Justice seems willing to adopt.[65] On September 2023, Federal Administrative Court in Leipzig confirmed that statutory obligation of telecommunications providers to retain telecommunications traffic data in breach of EU law.[66]

---

65 'Data retention does not help on the darknet' (original in German: 'Im Darknet hilft Vorratsdatenspeicherung nicht'), Tageschau (23 September 2022) https://www.tagesschau.de/inland/interview-tagesschau24-buschmann-101.html

66 Federal Administrative Court in Leipzig, 'Statutory obligation of telecommunications providers to retain telecommunications traffic data in breach of EU law' (original in German: 'Gesetzliche Verpflichtung der Telekommunikationsanbieter zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten unionsrechtswidrig'), Press release no 66/2023 (07 September 2023) https://www.bverwg.de/de/pm/2023/66 https://www.bverwg.de/de/pm/2023/66

GREECE

Greece implemented the EU Data Retention Directive 2006/24 via Law 3917/2011.[67] Following the invalidation of the Directive by the CJEU, the law was never revised nor invalidated. A law-making committee was set up in 2014 to address the CJEU judgment but did not produce any results, and stopped its operations in 2019.[68]

LEGAL BASIS	PURPOSES	CATEGORIES OF DATA	RETENTION PERIOD	ACCESS
Law 3917/2011 Law 5005/2022, Arts 4-6	N/A	Subscriber data Traffic data, Location data, IP addresses, Device identifiers (e.g. IMSI and EMEI numbers)	1 year	Police, intelligence agencies, judiciary (requires a court order)

Commentary

The law provides for blanket data retention without providing any indication regarding the reasons and basis for imposing such obligation. It is vague and all-encompassing providing limited details compared to similar laws in Belgium or Germany for instance. It provides limited safeguards and human rights protections. On the contrary, there are certain protections in place for accessing this data. Metadata are protected by the confidentiality of communications, under Law

67 Incorporation of Directive 2006/24/ec of the European parliament and of the council of 15 march on data retention generated or processed in connection with the provision services available to the public electronic communications or public communications networks and for the modification Directive 2002/58/EC, Law no 3917 (21 February 2021) http://www.adae.gr/fileadmin/docs/nomoi/nomoi/Nomos__3917_2011_diatirisi_dedomenon.pdf

68 Homo Digitalis, 'Preservation of Electronic Communications Metadata: The European ghost that wants to be reincarnated' (original in Greek: 'Διατήρηση Μεταδεδομένων Ηλεκτρονικών Επικοινωνιών: Το ευρωπαϊκό φάντασμα που θέλει να πάρει ξανά σάρκα και οστά') (1 August 2019), https://www.homodigitalis.gr/posts/4048#1534226685934-ba4ecff6-5435

3918/2011 and case law of Greek courts.[69] Access to metadata is therefore subject to the same conditions as access to content data. Access is regulated by Law 5005/2022.70 The Hellenic Authority for Communication Security and Privacy (ADAE) supervises communications secrecy, under the ADAE Regulation (Law 3115/2003).71 The Greek Data Protection Authority (HDPA) also has supervisory powers over metadata retention, under Article 9 of Law 3917/2011 and the HDPA Regulation (Law 4624/2019).72

Data subjects can be informed that their metadata has been accessed, but only after 3 years from termination of access, and only if a council composed of 3 members (ADAE president and two prosecutors) authorize it.[73] Data subjects can also submit a request to ADAE to find out whether they have been under surveillance for serious crime matters.[74] At the moment of writing, there is an ongoing complaint to the Hellenic Data Protection Authority following a telecommunication company's refusal in 2019 to provide access to retained metadata.[75]

---

69 See in particular Decision 1593 of the Greek Supreme Court on Constitutional Matters (2016), https://ddikastes.gr/%CE%B1%CF%80%CF%8C%CF%86%CE%B1%CF%83%CE%B7-%CF%83%CF%84%CE%B5-1593-2016-%CE%B4-7%CE%BC-%CF%80%CE%B1%CF%81%CE%AC%CE%B2%CE%B1%CF%83%CE%B7-%CF%84%CE%B7%CF%82-%CE%BD%CE%BF%CE%BC%CE%BF%CE%B8%CE%B5%CF%83/

70 Procedure for lifting the confidentiality of communications, cybersecurity and personal protection of citizens' personal data (original in Greek: Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών), Law no 5002 (9 December 2022) https://www.kodiko.gr/nomologia/download_fek?f=fek/2022/a/fek_a_228_2022.pdf&t=37e0e295a762d4ed152bbded744bb917

71 Hellenic Authority for Ensuring Communications Secrecy (in Greek: Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών*) Law no 3115* ΦΕΚ Α΄ *47/27.2.2003,* https://www.kodiko.gr/nomothesia/document/174570/nomos-3115-2003

72 Hellenic Data Protection Authority (HDPA), measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions, Law no 462 ΦΕΚ Α΄ *137/29.8.2019,* https://www.dpa.gr/sites/default/files/2020-08/LAW%204624_2019_EN_TRANSLATED%20BY%20THE%20HDPA.PDF

73 Article 4, Enhancing publicity and transparency in the printed and electronic press Establishment of electronic registers of the printed and electronic press Provisions of the General Secretariat for Communication and Information and other urgent regulations (original in Greek: Ενίσχυση δημοσιότητας και διαφάνειας στον έντυπο και ηλεκτρονικό Τύπο Σύσταση ηλεκτρονικών μητρώων εντύπου και ηλεκτρονικού Τύπου Διατάξεις αρμοδιότητας της Γενικής Γραμματείας Επικοινωνίας και Ενημέρωσης και λοιπές επείγουσες ρυθμίσεις), Law no 5005/2022, ΦΕΚ Α 236/21.12.2022 https://www.kodiko.gr/nomothesia/document/847353/nomos-5005-2022

74 Article 6, Law no 5005/2022, *ibid.*

75 *E Chelioudakis v Vodafone Greece*, Case number 8/2019.

LEBANON

There is no specific legal framework imposing on telecommunication and internet service providers to generally and indiscriminately retain communications data in Lebanon. However in 2013, the Public Prosecutor's office issued an order to all ISPs and Internet cafés to retain all communications data for a period of 1 year.[76] The Electronic Transactions and Personal Data law (Law no 81/2018), that the Lebanese parliament passed in September 2018, does not address bulk data retention obligations.[77] On 4 October 2021, it was reported that the Lebanese Prime Minister formed a ministerial committee to "look into granting security agencies and armed forces full access to all telecommunications data".[78]

LEGAL BASIS	PURPOSES	CATEGORIES OF DATA	RETENTION PERIOD	ACCESS
2013 Order of the Public Prosecutor	N/A	• Subscriber data • IP addresses • Location • Traffic data • Protocols used in the process	1 year	• Law enforcement • Intelligence agencies • Judicial authorities Subject to authorization from the public prosecutor

76 SMEX, 'Lebanon: It's time to turn your international position on privacy into action at the national level' (10 September 2015) https://smex.org/lebanon-its-time-to-turn-your-international-position-on-privacy-into-action-at-the-national-level/

77 Electronic Transactions and Personal Data law (Law no 81/2018) https://cyrilla.org/entity/vrlqtpwf7ss?file=1542184412658sl42tsmzwad.pdf&page=3; Freedom House, 'Freedom on the Net 2023: Lebanon', https://freedomhouse.org/country/lebanon/freedom-net/2023 (hereinafter Freedom House, 'Freedom on the Net 2023: Lebanon'); PI, State of Privacy Lebanon (27 January 2019) https://privacyinternational.org/state-privacy/1081/state-privacy-lebanon#commssurveillance (hereinafter PI, 'State of Privacy Lebanon')

78 Waleed Ahmed and Abed Kataya, 'Referring Telecom Data to Security Agencies Breaches the Lebanese Law', SMEX (26 October 2021) https://smex.org/referring-telecom-data-to-security-agencies-breaches-the-lebanese-law/

Commentary

Apart from the absence of a clear legal framework to regulate the retention of data, the 2013 order of the Public Prosecutor's office was vague and broad, lacking any procedural safeguards and human rights protections. The order instructs "all landline and wireless internet service providers for homes and companies and from all cafés and stores providing their clients with devices through which they can access the Internet" to "do whatever it takes to activate and save all Internet log files going through their servers and routers, and prepare a periodical backup copy to save these files from being lost, for at least one year."[79] Some experts consider that the order was not within the Public Prosecutor's powers to make, as criminal procedure law requires that data retention be only taken as a preventative measure, limited in time and applicability, and directly linked to an ongoing case or investigation. [80]

The Electronic Transactions and Personal Data law, that the Lebanese parliament passed in September 2018, regulates the protection of personal data and imposes some limitations to data retention, has been criticised as it fails to adequately protect user data due to vague language, inadequate safeguards for user data, and the lack of an independent oversight authority.[81]

Yet as of May 2022, it was reported that the two main mobile service providers in Lebanon, both Alfa and Touch, were owned by the state, and no tender was launched to change the status of the situation.[82] The companies were previously managed by private companies, but it was already since October 2020 that that government has functionally controlled the mobile telecommunications sector.[83] State ownership of the companies raises additional concerns in relation to the ability of state authorities to access this data.

---

79 PI, 'State of Privacy Lebanon', note 78.

80 SMEX, 'Lebanon: It's time to turn your international position on privacy into action at the national level' (10 September 2015) https://smex.org/lebanon-its-time-to-turn-your-international-position-on-privacy-into-action-at-the-national-level/

81 PI, 'State of Privacy Lebanon', note 78.

82 Freedom House, 'Freedom on the Net 2023: Lebanon', note 78.

83 "About Us," Touch, https://www.touch.com.lb/autoforms/portal/touch/about-touch/who-we-are/about-us; Alfa, "About Alfa", https://web.archive.org/web/20170216014412/https://www.alfa.com.lb/aboutus/companyinfo.aspx

MEXICO

The 2014 Federal Telecommunications and Broadcasting Law (FTB)[84] serves as the primary legal framework governing data retention in Mexico and articles 189 and 190 – whose constitutionality has been challenged[85] – impose bulk data retention obligations. As of now, the Supreme Court has not declared bulk data retention unconstitutional though.

In 2021, the Mexican Congress introduced the National Registry of Mobile Telephony Users, commonly called PANAUT.[86] This initiative aimed to establish a comprehensive database of individuals who subscribe to mobile telephone services in Mexico, in addition to the information already collected by service providers under articles 189 and 190. PANAUT officially became operational on 16 April 2021, following the publication of the law's reform. The intention was for the Federal Institute of Telecommunications (FIT) to oversee this registry. However, it was suspended in April 2022 after being deemed unconstitutional by the Supreme Court.[87]

84 Federal Telecommunications and Broadcasting Law (14 July 2014) https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf

85 See among others, R3D, 'Frequently asked questions on the unconstitutionality of articles 189 and 190 of the #TelecomLaw' (original in Spanish: Preguntas frecuentes sobre la inconstitucionalidad de los artículos 189 y 190 de la #LeyTelecom') (14 April 2016), https://r3d.mx/2016/04/14/preguntas-frecuentes-sobre-la-inconstitucionalidad-de-los-articulos-189-y-190-de-la-leytelecom/

86 The amendment was made by adding Chapter I BIS: 'National Register of Mobile Telephony Users' (original in Spanish: *'Del Padrón Nacional de Usuarios de Telefonía Móvil'*) and by modifying articles 189 and 190.

87 Supreme Court, action of unconstitutionality 82/2021 and its accumulated 86/2021, https://www2.scjn.gob.mx/juridica/engroses/cerrados/Publico/Proyecto/AI82_2021y86_2021acumuladaPL.pdf

LEGAL BASIS	PURPOSES	CATEGORIES OF DATA	RETENTION PERIOD	ACCESS
Federal Telecommunications and Broadcasting Law, Art 190	Efficiently collaborate with the competent authority to perform acts of investigation per the applicable provisions in security, enforcement, and justice administration	• Name, denomination, or company name and address of the subscriber • Type of communication (voice transmission, voicemail, conference, data), supplementary services (including call forwarding or call transfer) or messaging or multimedia services used (including short message services, multimedia and advanced services) • Data necessary to trace and identify the origin and destination of mobile telephony communications: destination number, modality of lines with contract or tariff plan, as in the modality of prepaid lines • Data necessary to determine the date, time, and duration of the communication, as well as the messaging or multimedia service • The date and time of the first activation of the service and the location tag (cell identifier) from which the service was activated must be kept • If applicable, identification and technical characteristics of the devices, including, among others, the international manufacturing identity codes of the equipment and the subscriber • The digital location of the geographic positioning of the telephone lines	2 years	Security and law enforcement agencies. Article 189 establishes that service providers are obliged to comply with all written, founded, and motivated orders from the competent authority in the terms established by law. However, the National Criminal Procedure Code and the Constitution establish that for access to the intervention of communications, it is necessary to have a judicial order. Metadata is considered communication under the Mexican legal system.

Commentary

The FTB imposes onerous data retention obligations that are both excessive in duration and indiscriminate in their application, encompassing all mobile phone users. The Supreme Court has taken commendable action by deeming the National Registry of Mobile Telephony Users, commonly (PANAUT) that was established in 2021 unconstitutional. It also underscores concerns about the lack of proportionality in comparison to less invasive alternatives. However, bulk data retention, as stipulated in Articles 189 and 190, remains in force. This retention practice is regulated by some specific Guidelines[88] adopted by the FIT. Specifically, they envision two working groups formed by authorities, the FIT and the service providers. Those groups should follow up on the telecommunication sector's implementation of these rules and the relevant technological evolution.[89] Yet they are lacking key procedural safeguards and human rights protections, such as judicial authorization and effective and independent oversight.

In particular, the FTB seems to imply that judicial authorization is unnecessary for accessing the data retained by these companies. Nevertheless, it is imperative to interpret these provisions comprehensively, considering the Constitution and other applicable laws. As per Article 252, Section III of the National Criminal Procedure Code, any form of private communication interception requires judicial authorization.[90] In Article 291,[91] private communications are defined as encompassing all information acquired while obtaining private communications, including communication identification data and information contained in documents, text, audio, images, or video files on any electronic device. So, in this sense, the access to metadata requires judicial authorization. This is compatible with Article 16 of the Constitution.[92]

---

88 Agreement whereby the Plenary of the Federal Telecommunications Institute issues the Guidelines for Collaboration in Security and Justice Matters and modifies the fundamental technical numbering plan (02 December 2015) https://dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015#gsc.tab=0

89 Chapter V, *ibid.*

90 Article 252, National Criminal Procedure Code (5 March 2014) https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP.pdf

91 Article 291, *ibid.*

92 Article 16, Political Constitution of the United Mexican States (5 February 1917), https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

SOUTH AFRICA

In South Africa, communications data and customer-related data is regulated by the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (RICA 2002).[93] The Cybercrimes Act 2020 has corresponding provisions that provide for law enforcement to issue preservation orders to ISPs, network providers or any other intermediaries in relation to communications and other data.[94] In 2021, the Constitutional Court of South Africa in the *amaBhungane* case, declared the data retention framework unconstitutional and order the government to introduce a new legal framework by the end of 2023.[95] The modifications are at the time of writing negotiated before the parliament.[96]

93 Act 70 of 2002, https://www.gov.za/sites/default/files/gcis_document/201409/a70-02.pdf

94 Cybercrimes Act, Act No 19 of 2020, https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf

95 See PI, 'amaBhungane and Sole challenge', https://privacyinternational.org/legal-action/amabhungane-and-sole-case-south-africa

96 See below end of this section.

LEGAL BASIS	PURPOSES	CATEGORIES OF DATA	RETENTION PERIOD	ACCESS
RICA 2002	N/A – all data must be retained	• Subscriber data • Traffic data • Location data • IP addresses "Communication-related information" defined as "switching, dialing or signaling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system"	3-5 years for communications data (note this is one of the longest mandatory data retention periods in the world)	Access to retained data is subject to authorization from a judge or magistrate through a subpoena or direction.
RICA 2002, ss.7-8	Prevention of serious injury or loss of life	Any data	N/A	Law enforcement can intercept or request emergency interception from ISPs (although they must get post-facto judicial approval)
Cybercrimes Act 2020 s.41-43	Finding evidence of any suspected offence	Content data and other electronic evidence	90 days	Police officials can issue a preservation order to the ISP while seeking a court order, as can magistrates and judges of the High Court – but the data can only be disclosed upon a court order

Commentary

The data retention period mandated by RICA 2002 is one of the longest in the world (3-5 years) – and although legally challenged in 2021, the Constitutional Court was not persuaded that it was unjustifiably long.[97] It did however require stricter safeguards around law enforcement access to retained data, for example that law enforcement seeking an interception warrant from a judge must disclose whether their target is a practising journalist or lawyer – but this only applies to procedures under RICA 2002, not to the more commonly used procedures under criminal law.

RICA 2002 applies to all ISPs, defined as "any person who provides access to, or any other service related to, the Internet to another person, whether or not such access or service is provided under and in accordance with an electronic communication service licence issued to the first mentioned person under Chapter 3 of the Electronic Communications Act". In practice however, the relevant regulations that govern data retention obligations have only been issued for mobile and fixed line operators, and no regulations have been issued that stipulate data retention for ISPs. It is not clear from publicly available information whether mobile network operators, who are all also ISPs, use the same data retention practices for their Internet and telephony services – although legal advisors to the ISP industry have previously recommended only retaining internet data that is necessary for billing and service provision until the relevant RICA regulations come into force.

There is no specific mechanism under RICA 2002 for individuals to be informed or complain about retention of or access to their data. However, they can complain to the Information Regulator (South Africa's data protection authority) about the processing of their data. Also, there are no oversight mechanisms relating to retention. Judicial authorities can only intervene as oversight mechanisms when law enforcement seeks to access or has accessed data. At the moment of writing, there is no time limit to the retention of data that has been intercepted or accessed

97 amaBhungane Centre for Investigative Journalism NPC and another v Minister of Justice and Correctional Services and Others; Minister of Police v amaBhungane Centre for Investigative Journalism NPC and others (CCT 278/19, CCT 279/19) [2021] ZACC 3, 2021 (4) BCLR 349 (CC), 2021 (3) SA 246 (CC) (4 February 2021) http://www.saflii.org/za/cases/ZACC/2021/3.html

by law enforcement or intelligence agencies – but in 2021, in the *amaBhungane* case, the Constitutional Court of South Africa ordered Parliament to amend the law to implement such safeguards.[98]

In response to this judgment, Parliament issued a revised version of the law on 25 August 2023, as detailed in Government Gazette 49189 (currently approved by Parliament and waiting to be signed into law).[99] As raised during consultation, the proposed legislation continues to raise several critical issues as the proposed draft falls short of international human rights standards, including in relation to bulk data retention obligations.[100] For instance, the updated law introduced Article 37A, focusing on data management. The provided text delineates procedures for managing data obtained through the interception of communications, that would potentially also apply to telecommunication providers, lacks a specific time limit, only indicating the necessity of establishing such limits.

TUNISIA

In Tunisia, Decree-law n°2022-54 of 13 September 2022 (*Décret-loi*) regulates data retention.[101] Under this law, retention obligations apply to both electronic telecommunications providers and Internet services providers. The regime provides for the indiscriminate and generalised retention of traffic and location data.

98 *ibid.*

99 Regulation of Interception of Communications and Provision of Communication-related Information Amendment Bill (B28-2023) https://pmg.org.za/bill/1172/

100 PI, 'PI's response on proposed draft RICA Bill' (1 November 2023) https://privacyinternational.org/advocacy/5153/pis-response-proposed-draft-rica-bill

101 Decree-Law no. 2022-54 of 13 September 2022 on combating offences relating to information and communication systems (original in French : Décret-loi n° 2022-54 du 13 septembre 2022, relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication), Journal Officiel de la République Tunisienne, N°103 (13 Septembre 2022), p 2654, https://www.pist.tn/jort/2022/2022F/Jo1032022.pdf

LEGAL BASIS	PURPOSES	CATEGORIES OF DATA	RETENTION PERIOD	ACCESS
Decree-law no. 2022-54 of 13 September 2022	Safeguarding public safety Safeguarding national defence Abiding to provisions imposed by the judiciary	Data allowing the identification of users of the service Data relating to traffic flow Data relating to the device used in the communication Data related to the geographical location of the user Data relating to the access and use of "protected value-added content" (not defined)	Retention period not specified provided: • fixed by ministerial order, subject to being no less than 2 years from the date of the data collection	Persons authorised to demand the transmission of the retained data: • the public prosecutor • the investigating judge • police officers
		The interception of communications includes: • obtaining access data • listening to or accessing their content • reproducing or recording them Access data: data that help identify the type of service, the source of the communication, its destination, its transmission network, time, date, volume and duration of the communication		In cases where the necessity of the investigation so requires, the public prosecutor or the investigating judge may resort to intercepting the communications of suspects following a written decision or a detailed report by a police officer.
				The authority accessing retained data is required to report on the access or collection or interception or processing operations that were carried out. Such report must contain in particular: • The authority that ordered the technical processing of retained data • The technical measures that were taken to execute the order and the type of assistance it received from the service provider • The technical measures taken to preserve the data collected and ensure its integrity and authenticity • Date and time of the start and end of the operations

Commentary

The Decree-law mandates general and indiscriminate data retention by telecommunication service providers and introduces overly broad data access and interception powers for state authorities. The Tunisian legal framework appears to provide for some safeguards in relation to certain aspects, as for instance it sets conditions for persons authorized to access information regarding legally privileged information. Yet and despite its general reference to human rights law, it does not include procedural safeguards, such as a right to be notified of surveillance measures and a right to appeal. Further, Tunisia's data retention regime provides for severe prison sentences and heavy fines should any service provider violate their obligations.[102]

What is most concerning is that those far-reaching investigatory powers are introduced in the law to authorize investigations into acts that constitute protected online speech rather than serious crimes in conformity with international human rights law. The Decree-law includes measures like the ban on spreading misinformation, which limit legitimate freedom of speech. These measures are being employed to take legal action against journalists, human rights defenders, and those who criticize the government.[103] Many civil society organisations have raised the alarm regarding the legislation compliance with human rights standards, underlining that the draconian framework threatens democratic principles and providing a basis for cracking on civil society and dissent.[104]

---

102 For instance, if the service provider (the company) that does not comply with the obligation to retain data, they face a penalty of 1 year imprisonment and a fine of 10.000 dinars. If the service provider made a profit by disregarding data retention obligations, they face a fine of 50.000 dinars. A court may also ban the company's activities for up to five years or even order its dissolution. In addition, the law provides that anyone who intentionally violates the confidentiality of procedures relating to the collection, interception, or recording of traffic flow data or its contents faces 3 years imprisonment and a fine of 20.000 dinars.

103 Article 19, 'Tunisia: Cybercrime law is a grave threat to freedom of expression' (30 March 2023) https://www.article19.org/resources/tunisia-cybercrime-law-is-threat-to-free-expression/

104 See also, SMEX, 'Tunisia: Decree-Law No. 54 puts freedom of the press in jeopardy' (25 October 2022) https://smex.org/decree-law-no-54-in-tunisia-freedom-of-the-press-in-jeopardy/; International Commission of Jurists, 'Tunisia: Repeal Draconian Cybercrime Decree' (20 September 2020) https://www.icj.org/tunisia-repeal-draconian-cybercrime-decree/

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).