PRIVACY INTERNATIONAL

Informe de actor interesado
Examen Periódico Universal
30º período de sesiones - Colombia

El derecho a la intimidad en Colombia

Presentado por Dejusticia, Fundación Karisma y Privacy International

Octubre 2017

El derecho a la intimidad en Colombia

Octubre 2017

PRIVACY INTERNATIONAL

www.privacyinternational.org

I. Introducción

1. Este informe de terceras partes interesadas es una contribución escrita presentada por Dejusticia, Fundación Karisma y Privacy International (PI). Dejusticia es una organización de derechos humanos colombiana que brinda conocimientos especializados sobre derechos humanos. Fundación Karisma es una organización de la sociedad civil colombiana que busca dar respuesta a las oportunidades y a las amenazas que surgen en el contexto de la *tecnología para el desarrollo* para el ejercicio de los derechos humanos. PI es una organización de derechos humanos que trabaja para impulsar y promover el derecho a la intimidad y luchar contra la vigilancia en todo el mundo.

2. Dejusticia, Fundación Karisma y Privacy International desean plantear ciertas preocupaciones sobre la protección y la promoción del derecho a la intimidad con el propósito de que sean consideradas en el próximo examen de Colombia en la 30° periodo de sesiones del Grupo de Trabajo sobre el Examen Periódico Universal.

II. El derecho a la intimidad

3. La intimidad es un derecho humano fundamental, consagrado en numerosos instrumentos internacionales de derechos humanos.[1] Es esencial para la protección de la dignidad humana y constituye la base de cualquier sociedad democrática. También respalda y refuerza otros derechos, como la libertad de expresión, información y asociación.

4. Las actividades que restringen el derecho a la intimidad, como la vigilancia y la censura, solo pueden justificarse cuando han sido establecidas por la ley, son necesarias para lograr un objetivo legítimo y son proporcionales al objetivo perseguido.[2]

[1] Declaración Universal de Derechos Humanos artículo 12, Convención de las Naciones Unidas sobre Trabajadores Migratorios artículo 14, Convención de la ONU párr la Protección del Niño artículo 16, Pacto Internacional de Derechos Civiles y Políticos artículo 17; convenciones regionales incluyendo el artículo 10 de la Carta Africana sobre los Derechos y el Bienestar del Niño, el artículo 11 de la Convención Americana sobre Derechos Humanos, el artículo 4 de los Principios sobre Libertad de Expresión de la Unión Africana, el artículo 5 de la Declaración Americana de los Derechos y Deberes del Hombre, el artículo 21 de la Carta Árabe de Derechos Humanos y el artículo 8 del Convenio Europeo párr la Protección de los Derechos Humanos y de las Libertades Fundamentales; Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información, los Principios de Camden sobre Libertad de Expresión y la Igualdad.

[2] Declaración Universal de Derechos Humanos artículo 29; Comentario general No. 27, adoptado por el Comité de Derechos Humanos en virtud del artículo 40, párrafo 4, del Pacto Internacional de Derechos Civiles y Políticos, CCPR/C/21/Rev.1/Add.9, 2 de noviembre de 1999; Ver también Martin Scheinin, "Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo", 2009, A/HRC/17/34.

5. Varios instrumentos internacionales consagran los principios de la protección de datos,[3] y muchas legislaturas nacionales han incorporado esos principios a la legislación nacional.[4]

III. Seguimiento al EPU anterior

6. Durante el examen anterior de Colombia en el segundo ciclo en 2013, no se mencionó explícitamente el derecho a la intimidad en el contexto de la protección de datos y la vigilancia de las comunicaciones en el Informe Nacional presentado por el gobierno de Colombia o en el informe del Grupo de Trabajo.

7. Sin embargo, el informe de compilación del ACNUDH planteó la cuestión de que "el Grupo de Trabajo sobre las Desapariciones Forzadas o Involuntarias consideró que Colombia aún carecía de una política para depurar la Fuerza Pública y otros organismos de seguridad e inteligencia del Estado de sus vínculos con el paramilitarismo".[5] Asimismo, el informe[6] resaltó las preocupaciones expresadas por el Comité de Derechos Humanos de la ONU respecto a las políticas y prácticas ilegales de vigilancia de las comunicaciones en 2012,[7] las cuales también fueron planteadas en el último examen del Comité en 2016.[8]

8. Adicionalmente, los diferentes actores interesadas plantearon la cuestión de la vigilancia ilegal de los defensores de los derechos humanos y también la protección de la libertad de expresión en línea.[9]

9. Finalmente, las delegaciones gubernamentales hicieron numerosas menciones y recomendaciones sobre la protección de los defensores de los derechos humanos y los periodistas para denunciar e investigar abusos y violaciones de los derechos humanos.[10]

IV. Normas nacionales relacionadas con la intimidad

10. El ordenamiento jurídico colombiano prevé una serie de protecciones fundamentales del derecho a la intimidad.

3 Ver el Convenio del Consejo de Europa párr la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (No. 108), 1981; las Directrices de la Organización párr la Cooperación y el Desarrollo Económicos sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales (1980); y los Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales (resolución 45/95 y E/CN.4 /1990/72 de la Asamblea General). A diciembre de 2013, 101 países habían promulgado legislación sobre la protección de datos.

4 A diciembre de 2013, 101 países habían promulgado legislación sobre la protección de datos. Ver: David Banisar,National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (28 de enero de 2014). Disponible en SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

5 A/HRC/WG.6/16/COL/2, párr. 30

6 Ibid, párr. 18

7 CCPR/C/COL/CO/6, párr. 27

8 CCPR/C/COL/CO/7, párr. 32-33

9 A/HRC/WG.6/6/COL/3, párrafos 14 y 54

10 A/HRC/24/6. Ver recomendaciones: 116.19, 116.73, 116.74, 116.75, 116.76, 116.77, 116.80, 116.81, 116.82, 116.83, 116.85,116.110

11. El artículo 15 de la Constitución de 1991 establece que toda persona tiene derecho a la intimidad personal y familiar. Reza:
"La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley".

12. El artículo 250 de la Constitución confiere a la Fiscalía General de la Nación la facultad de adelantar incautaciones, decomisos e interceptaciones de comunicaciones sin autorización judicial previa. El artículo 235 del Código de Procedimiento Penal estipula las condiciones en las que la Procuraduría General puede ordenar la interceptación de comunicaciones. La interceptación sin orden judicial, salvo la facultad de la Fiscalía General para realizar tal intercepción, constituye un delito conforme al Código Penal.

13. La Ley 1266 de 2008 protege los datos personales financieros en Colombia. Originalmente esta ley pretendía ser el marco jurídico general aplicable al tratamiento de datos personales. Después de ser revisada por la Corte Constitucional (Sentencia C-1011 de 2008), su alcance se redujo solo a la información financiera, crediticia, comercial y de servicios (y la información proveniente del exterior como la que está relacionada con riesgo financiero y evaluación de riesgo crediticio ("Datos financieros personales").

14. En 2012, el Congreso de Colombia promulgó su propia legislación general de protección de datos: la Ley 1581 de 2012, que constituye el marco jurídico general aplicable al tratamiento de datos personales. Esta ley fue revisada por la Corte Constitucional en la Sentencia C-748 de 2011, y regulada por el Decreto 1377 de 2013.

V. Obligaciones internacionales

15. Colombia ha ratificado varios tratados internacionales de derechos humanos con repercusiones en materia de intimidad. Ha ratificado el Pacto Internacional de Derechos Civiles y Políticos (PIDCP), que defiende el derecho a la intimidad en su artículo 17. El Comité de Derechos Humanos ha observado que los Estados Partes en el PIDCP tienen la obligación positiva de "adoptar medidas legislativas y de otra índole para hacer efectivas la prohibición de esas injerencias y ataques y la protección de este derecho [intimidad]".

16. El 28 de mayo de 1973, Colombia ratificó la Convención Americana sobre Derechos Humanos o el "Pacto de San José de Costa Rica" (la "Convención Americana") que en su artículo 11 establece que "nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación".

17. Además, Colombia es parte de la Convención internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares, y la Convención internacional para la protección de todas las personas contra las desapariciones forzadas.

18. Todos estos tratados de derechos humanos ratificados por Colombia hacen parte de la Constitución de Colombia en virtud del artículo 92 de la misma, que les confiere el rango superior de norma constitucional de conformidad con el parágrafo 13.

VI. Áreas de preocupación

i) Fines demasiado amplioss

19. Aparte de las facultades de vigilancia relacionadas con los procesos de investigación penal y las de la Fiscalía General de la Nación, Colombia ha promulgado una Ley de Inteligencia y Contrainteligencia (Ley Estatutaria No. 1621 de 2013). Esta ley regula las actividades de inteligencia y contrainteligencia, incluido el "monitoreo del espectro electromagnético".

20. Los fines para los cuales se puede obtener información en los términos establecidos en el artículo 4 de la Ley No. 1621 de 2013, son demasiado amplios y definidos vagamente, e incluyen: garantizar la seguridad nacional, la soberanía, la integridad territorial, la seguridad y defensa de la Nación, la protección de las instituciones democráticas y los derechos de los residentes y ciudadanos colombianos y la protección de los recursos naturales e intereses económicos de la Nación.

21. Esto fines tan amplios permiten una interpretación expansiva de los casos en que se puede efectuar la vigilancia de las comunicaciones, lo cual no cumple los tests de legalidad, necesidad y proporcionalidad.

ii) Ausencia de una definición de “monitoreo del espectro electromagnético”

22. El artículo 17 de la Ley de Inteligencia se titula "Monitoreo del espectro electromagnético e interceptaciones de comunicaciones privadas" y distingue el monitoreo del espectro electromagnético para fines de inteligencia y contrainteligencia, con el propósito de mantener la seguridad nacional, de la interceptación de comunicaciones. Pero el *monitoreo* del espectro electromagnético no está definido en la ley colombiana.

23. Al no existir una definición, *monitorear* el espectro electromagnético podría incluir el análisis y monitoreo de los correos electrónicos, mensajes de texto y las llamadas telefónicas que se transmitan a través del espectro electromagnético. Esos actos constituyen una *interceptación* de la comunicación y, por consiguiente, interfieren con la intimidad de la persona que envía y recibe la información.

24. De conformidad con el artículo 17, las interceptaciones de comunicaciones no están autorizadas bajo la Ley de inteligencia, sino que únicamente pueden realizarse conforme a los requisitos de ley establecidos en el Código de Procedimiento Penal, de manera selectiva. Sin embargo, la afirmación de que el *monitoreo* no constituye una interceptación de comunicaciones lleva a una importante laguna jurídica que plantea serias preocupaciones respecto a la protección del derecho a la intimidad.

iii) "Monitoreo del espectro electromagnético" sin autorización judicial previa

25. A la luz de lo anterior, la expresión "el monitoreo no constituye una interceptación de comunicaciones" con arreglo al artículo 17 de la Ley de Inteligencia no reconoce que el monitoreo del espectro electromagnético constituye una interferencia con la intimidad de las comunicaciones.

26. Al no exigir que el *monitoreo* del espectro electromagnético esté sujeto a normas iguales o similares a las que regulan la interceptación de comunicaciones conforme al Código de Procedimiento Penal, la Ley de Inteligencia no brinda protección contra las injerencias en las comunicaciones privadas.

27. Este vacío normativo es particularmente problemático dado el tipo de tecnologías de vigilancia utilizadas por las fuerzas de seguridad y del orden público colombianas que fueron señaladas en otros apartes de nuestra contribución. Como se señaló en las Observaciones finales sobre el séptimo informe periódico de Colombia, existe la preocupación de "injerencias en las comunicaciones privadas realizadas a través del espectro electromagnético que no estén sujetas a una estricta evaluación de legalidad, necesidad y proporcionalidad".[11]

iv) La Policía goza de amplias facultades sin que existan controles apropiados

28. En enero de 2017, entró en vigencia el Código Nacional de Policía y Convivencia para Vivir en Paz. Este nuevo Código otorga amplias facultades a la policía sin establecer controles apropiados a la discreción de la misma. Incluye varias disposiciones que tienen repercusiones particularmente negativas con respecto al derecho a la intimidad y su interpretación colectiva, lo que puede conducir a un estado de vigilancia.

29. En primer lugar, el artículo 32 contiene una definición demasiado estrecha de intimidad. Al definir el derecho a la intimidad como el derecho de las personas "a satisfacer sus necesidades y desarrollar sus actividades en un ámbito que le sea exclusivo y por lo tanto considerado como privado", la norma parece confundir el derecho a la intimidad con el derecho al libre desarrollo de la personalidad y con el derecho a la inviolabilidad del hogar.

30. Por lo tanto, al vincular el derecho a la intimidad con la existencia de espacios físicos privados, excluye de la protección de la intimidad a las personas o bienes

[11] CCPR/C/COL/CO/7, párr. 32-33

(como automóviles, o dispositivos electrónicos como computadoras portátiles o teléfonos celulares) que estén ubicado en lugares públicos, incluyendo bares, restaurantes, etc., lo que a su vez deja en una zona gris jurídica a los actos privados que ocurran en el espacio público.

31. Por el contrario, el artículo 139 define el espacio público de una manera muy amplia, incluyendo especialmente "el espectro electromagnético".

32. El resultado combinado de estas definiciones es de gran importancia para la protección de la intimidad, particularmente cuando se considera que el artículo 237 podría interpretarse en el sentido de que las comunicaciones que viajan a través del espectro electromagnético quedarían excluidas de la protección de la intimidad.

33. Por último, el nuevo Código de Policía parece no tener en cuenta los complejos cambios tecnológicos que afectan a las comunicaciones moderna. Por lo tanto, no está claro cómo se protege la intimidad de las comunicaciones digitales y de los espacios en línea teniendo en cuenta las definiciones muy restrictivas de intimidad y espacio público consagradas en el Código.

34. Este defecto de la ley fue planteado por el Comité de Derechos Humanos, que destacó la preocupación de que el nuevo Código de Policía "*prevea una definición muy amplia de lo que es espacio público, que incluye el espectro electromagnético, y que toda la información y los datos recolectados en los espacios públicos sean considerados públicos y de libre acceso (art. 17)*".[12]

v) Las capacidades de las tecnologías de vigilancia que operan fuera del ordenamiento jurídico

35. El sistema de interceptación de comunicaciones más conocido de Colombia se llama Esperanza. La Fiscalía General de la Nación administra la plataforma, la cual puede obtener los datos y el contenido de las llamadas de telefonía móvil y fija. Varios organismos de orden púbico en Colombia utilizan este sistema para obtener pruebas para las investigaciones penales y los enjuiciamientos. Se basa en la colaboración de los operadores de telecomunicaciones, que están obligados, de conformidad con el ordenamiento colombiano, a cooperar con las solicitudes de interceptación de las autoridades competentes.[13]

36. En 2007, la Policía estableció un sistema con capacidades de vigilancia aún más amplias, conocido como la Plataforma Única de Monitoreo y Análisis (PUMA). A diferencia de Esperanza, el sistema PUMA está directamente relacionado con la infraestructura de red del proveedor de servicio, lo que potencialmente podría permitir que el sistema intercepte las comunicaciones de todas las personas que pasen por esta red y las dirija a las instalaciones de monitoreo de las fuerzas de orden público sin ninguna facilitación adicional del proveedor del servicio. Las

[12] CCPR/C/COL/CO/7, párr. 32

[13] Privacy Internacional, Shadow State: Surveillance, Law and Order in Colombia, agosto de 2015. Disponible en: https://privacyinternational.org/report/991/shadow-state-surveillance-law-and-order-colombia

empresas israelíes Verint y posteriormente NICE proporcionaron la tecnología operativa de PUMA.

37. Una rama de la Policía, la DIPOL (Dirección de Inteligencia Policial), también emplea un sistema de vigilancia masiva que se denomina Sistema Integrado de Grabación Digital (SIGD). La interceptación a través de SIGD, al igual que en el caso de PUMA, se realiza en masa y sin la asistencia de los proveedores de servicio.

38. Si bien el Decreto 1704 (2012) exige que los proveedores de telecomunicaciones configuren su infraestructura para permitir el "acceso a la captura del tráfico" con fines de investigación penal, no hay ninguna disposición expresa que permita o prohíba las medidas de vigilancia en masa como PUMA o SIGD en el marco normativo vigente que regula la vigilancia de comunicaciones en Colombia.

vi) Despliegue de tecnologías de vigilancia intrusivas

39. Existen informes que indican que las autoridades colombianas han adquirido tecnologías de vigilancia intrusivas.

40. Hacking Team produce un sistema de intrusión que fue adquirido por la policía colombiana.[14] El Sistema de Control Remoto (RCS por sus siglas en inglés) de la compañía se puede usar para tomar el control de una computadora y de dispositivos móviles sin ser detectado por el usuario ya que está diseñado para eludir los programas de antivirus y el cifrado comunes. Al infectar el dispositivo del blanco de la vigilancia, el paquete de RCS puede capturar datos en el dispositivo del blanco, encender y apagar cámaras web y micrófonos, copiar archivos y contraseñas que hayan sido digitados. Además, puede recoger, modificar y/o extraer datos del dispositivo objeto sin que sea detectado. En este sentido, es una forma particularmente intrusiva de vigilancia electrónica, dada la información personal que se puede obtener de dicho acceso.

41. Una investigación de 2014 del Citizen Lab en la Universidad de Toronto concluyó que desde 2012 estas tecnologías han sido identificadas y asociadas con ataques contra periodistas, activistas y defensores de los derechos humanos, y reveló evidencia que confirma el presunto despliegue de esas tecnologías en por lo menos 21 países, incluyendo Colombia.[15]

42. En 2014, Hacking Team tenía un ingeniero de campo radicado en Colombia y un contrato activo con la policía colombiana. De acuerdo con la investigación de Privacy International[16] Hacking Team tenía un contrato activo con la policía colombiana en 2014. A pesar de esta poderosa evidencia del despliegue de los productos de malware ofensivo de Hacking Team, la policía colombiana

[14] Privacy Internacional, Shadow State: Surveillance, Law and Order in Colombia, agosto de 2015. Disponible en: https://privacyinternational.org/report/991/shadow-state-surveillance-law-and-order-colombia

[15] The Citizen Lab, Mapping Hacking Team's "Untraceable" Spyware, 17 de febrero de 2014. Disponible en: https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/

[16] Privacy Internacional, Shadow State: Surveillance, Law and Order in Colombia, agosto de 2015. Disponible en: https://privacyinternational.org/report/991/shadow-state-surveillance-law-and-order-colombia

negó toda relación directa con Hacking Team, admitiendo únicamente vínculos contractuales con una empresa colombiana llamada Robotec,[17] la cual es un intermediario para la distribución de dichos productos. Sin embargo, el documento fechado julio de 2015 sobre Hacking Team que fue filtrado puso de manifiesto que la policía colombiana tuvo contacto directo con Hacking Team para activar los productos de malware ofensivo que compraron en los primeros meses de 2015.

43. De acuerdo con lo dispuesto en el artículo 269A del Código Penal colombiano, el *hackeo* ("acceso abusivo a un sistema informático") es un delito, y por lo tanto, ante la falta de una ley que regule expresamente su uso con fines de vigilancia, es una forma de vigilancia extralegal que es ilegal conforme a la ley colombiana. La intrusión en la intimidad que implica y el riesgo para la seguridad de las comunicaciones genera profundas inquietudes con respecto a los derechos humanos. Como forma de vigilancia gubernamental, el hackeo presenta amenazas únicas y graves tanto para la intimidad como para la seguridad. Tiene el potencial de ser mucho más intrusivo que cualquier otra técnica de vigilancia, permitiendo el acceso del gobierno a nuestros dispositivos personales y toda la información íntima que almacenan. También permite que el gobierno controle la funcionalidad de nuestros dispositivos, facilitando la vigilancia en tiempo real a través del micrófono, la cámara web y la tecnología de localización basada en GPS de los dispositivos, o permitiendo la alteración, creación o eliminación de datos. Al mismo tiempo, el hackeo tiene el potencial de comprometer no solo la seguridad de los sistemas específicos, sino también al Internet en general.

44. Adicionalmente, muchas empresas ofrecen equipos de monitoreo móvil, también conocidos como "IMSI catcher" en Colombia, según una investigación de Privacy International.[18] Un IMSI Catcher realiza interceptación al presentarse como una estación base en la red móvil: la estación a la que se conecta un teléfono cuando desea hacer una llamada o enviar un mensaje. Una vez conectado a la estación base del IMSI Catcher, es posible monitorear el funcionamiento del teléfono: las llamadas de voz que se realizan, los mensajes que se envían y la ubicación del teléfono y recuperar identificadores únicos del dispositivo como sus números IMEI e IMSI.

45. Spectra Group, con sede en Nueva Zelanda, a través de la empresa colombiana Microtel Ltda. suministró su IMSI catcher Laguna a la Dirección de Inteligencia Policial (DIPOL) en septiembre de 2005. El sistema Laguna está diseñado para monitorear y registrar conversaciones y datos telefónicos en sistemas de comunicación móvil y puede ser de carácter móvil o ensamblarse en estaciones fijas.

46. Bulldog y Nesie, fabricados por la empresa británica de vigilancia Smith Myers, son otros dos IMSI catchers populares vendidos en Colombia. En 2010, el DAS se estaba preparando para comprar un sistema de interceptación Bulldog por

[17] Durán Núñez, DC, El software espía de la Policía, 11 de julio de 2015. El Espectador. Disponible en: https://www.elespectador.com/noticias/investigacion/el-software-espia-de-policia-articulo-571980

[18] Privacy Internacional, Shadow State: Surveillance, Law and Order in Colombia, agosto de 2015, págs. 42. Disponible en: https://privacyinternational.org/report/991/shadow-state-surveillance-law-and-order-colombia

más de US$250.000 y un sistema Nesie por más de US$320.000. La Fiscalía también planeaba comprar un sistema Bulldog por poco más de US$280.000, al igual que la seccional de la DIJIN de Bogotá. En 2014, la sucursal finlandesa de la empresa canadiense de telecomunicaciones Exfo exportó su IMSI catcher NetHawk F10 a Colombia.[19]

47. Los mecanismos de derechos humanos de la ONU han expresado su preocupación sobre el uso del hackeo con fines de vigilancia.[20] El Relator Especial de la ONU sobre libertad de expresión señaló en su informe de 2013 que "los programas informáticos ilegales invasivos como los troyanos o los mecanismos de interceptación a gran escala atentan seriamente contra las nociones tradicionales de vigilancia que no pueden conciliarse con la legislación en vigor sobre vigilancia ni con el acceso a la información privada (...) Desde la perspectiva de los derechos humanos, el uso de estas tecnologías es sumamente perturbador. Por ejemplo, los troyanos no solo permiten al Estado acceder a dispositivos, sino que también les permiten modificar, en forma inadvertida o deliberada, la información allí contenida. Esto atenta no solo contra el derecho a la intimidad y los derechos a la equidad procesal respecto del uso de estas pruebas en las actuaciones judiciales".[21]

vii) Informes de interceptaciones ilegales de comunicaciones privadas, incluyendo a periodistas y defensores de los derechos humanos

48. Los escándalos por la interceptación de comunicaciones (a veces denominadas por el término colombiano *chuzadas*) han sido una característica del contexto político de la seguridad en Colombia desde la década los noventa. Incluyen la vigilancia ilegal de políticos, jueces, periodistas y defensores de los derechos humanos y familias de personas desaparecidas.

49. En 2014, la revista semanal colombiana *Semana* informó que una unidad del ejército colombiano conocida con el nombre clave Andrómeda espió durante más de un año al equipo negociador del gobierno en las conversaciones de paz con la guerrilla FARC del país.[22]

50. Las historias de la interceptación ilegal de comunicaciones privadas dominan los relatos de desapariciones y asesinatos extrajudiciales. Diferentes organismos han estado involucradas en estas intercepciones ilegales, por ejemplo:

    - La interceptación ilegal de 2.500 líneas telefónicas por las unidades conjuntas del Ejército y la Policía, los Grupos de Acción Unificada por la Libertad Personal (GAULA), incluyendo a un grupo que representa a las familias de los desaparecidos, específicamente la Asociación de

19 Ibid

20 En 2017, el Comité de Derechos Humanos expresó su preocupación por el uso del hackeo con fines de vigilancia en Italia. Ver: Observaciones finales sobre el sexto informe periódico de Italia, Comité de Derechos Humanos, UN Doc. CCPR/C/ITA/CO/6 (28 de marzo de 2017)

21 Informe del Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, UN Doc. A/HRC/23/40, párr. 62 (17 de abril de 2013).]

22 Semana, ¿Alguien espió a los negociadores de La Habana?, 3 de febrero de 2014. Disponible en: http://www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/37607

Familiares de Detenidos- Desaparecidos (ASFADDES) entre muchas otras organizaciones de derechos humanos.[23]

- El despido de la DIPOL de once generales de la policía después de que se reveló que el organismo había interceptado las líneas telefónicas de influyentes políticos de oposición, periodistas, abogados y activistas.[24]

51. Sin embargo, el más conocido de los escándalos de interceptación involucra al Departamento Administrativo de Seguridad (DAS) y fue revelado por *Semana* en febrero de 2009. Grupos especiales de inteligencia estratégica del DAS efectuaron labores de vigilancia específica a aproximadamente 600 figuras públicas, incluyendo parlamentarios, periodistas, activistas y abogados de derechos humanos, y jueces, entre otros. Según los archivos recuperados en la investigación de la Fiscalía, el DAS interceptó llamadas telefónicas, tráfico de correo electrónico y listas de contactos internacionales y nacionales, utilizando esta información para elaborar perfiles psicológicos de los blancos y llevar a cabo la vigilancia física de los sujetos y sus familias, incluyendo los niños.[25]

52. La vigilancia de las comunicaciones fue fundamental en los abusos del DAS. Privacy International habló con personas sobre las cuales se confirmó que fueron objeto de la vigilancia del DAS y personas que tienen la firme convicción de que aún son blancos de la vigilancia electrónica estatal. Los documentos del DAS que fueron recuperados durante el escándalo de interceptación ilegal en 2009 contenían descripciones detalladas de los movimientos de los empleados y las familias del Colectivo de Abogados "José Alvear Restrepo" (CCAJAR), listas de sus contactos telefónicos y registran los esfuerzos del DAS de vincular números telefónicos con miembros del CCAJAR.[26]

53. Las líneas telefónicas del periodista Hollman Morris estuvieron bajo vigilancia casi constante. Más adelante, Morris tuvo que exiliarse en varias ocasiones. Claudia Duque, una abogada y periodista que antes trabajaba en el colectivo de abogados CCAJAR, sobrevivió a intentos de secuestro y recibió violentas y gráficas amenazas telefónicas de muerte; los archivos del DAS sobre ella tenían amplia evidencia de vigilancia física y de sus comunicaciones.[27] Tal era la escala de la interceptación ilegal que siete jueces de la Corte Suprema fueron recusados del juicio en 2011 del antiguo jefe del DAS porque la evidencia sugería que incluso ellos habían sido espiados ilegalmente.[28]

---

[23] "Informe Sobre Derechos Humanos: Colombia", Departamento de Estado de los Estados Unidos, 4 de marzo de 2002. Disponible en: http://www.acnur.org/t3/leadmin/scripts/doc.php?le=t3/uploads/media/COI_53

[24] El Espectador, El DAS-gate y las "chuzadas", vuelve y juega, 21 de febrero de 2009. Disponible en: http://www.elespectador.com/impreso/judicial/articuloimpreso120201-el-das-gate-y-chuzadas-vuelve-y-juega

[25] El Tiempo, Un 'manual' para seguir y acosar a las personas calificadas como opositores tenía el DAS, 13 de junio de 2009. Disponible en: http://www.eltiempo.com/archivo/documento/CMS-5436047

[26] Privacy Internacional, Shadow State: Surveillance, Law and Order in Colombia, agosto de 2015, págs. 53-54. Disponible en: https://privacyinternational.org/report/991/shadow-state-surveillance-law-and-order-colombia

[27] IFEX, Former security operatives charged in journalist's torture in Colombia, 18 de marzo de 2013. Disponible en: https://www.ifex.org/colombia/2013/03/18/security_charged/; Committee to Protect Journalists, Colombian Official convicted of "psychological torture" of journalist, 22 de diciembre de 2014. Disponible en: https://cpj.org/2014/12/colombian-of cial-convicted-of-psychological-tort.php

[28] Colombia Reports, 7 judges withdrawn from wiretap trial, 12 de agosto de 2011. Disponible en: http://colombiareports.com/7-supreme-court-judges-victimized-in-wiretap-scandal-withdrawn-from-trial/

54. En medio de escándalos, el DAS fue disuelto en octubre de 2011. Varios de los antiguos dirigentes del DAS fueron condenados por interceptación ilegal y delitos conexos. Fernando Tabares, antiguo director del DAS, fue condenado por las chuzadas ilegales a opositores al gobierno en 2010. Jorge Noguera y María del Pilar Hurtado, quienes lideraron el DAS en 2002 y 2008, son los funcionarios de más alto rango condenados por vigilancia ilegal. En 2011, se creó un nuevo organismo, la Dirección Nacional de Inteligencia (DNI), para dirigir el sector de inteligencia y contrainteligencia dentro de la estructura general del estado.

55. En las Observaciones finales sobre el séptimo informe periódico de Colombia, el Comité de Derechos Humanos de la ONU dijo que el gobierno debería "*acelerar las investigaciones relativas a las presuntas actividades ilegales de seguimiento presuntamente realizadas por funcionarios del antiguo Departamento Administrativo de Seguridad y garantizar que todos los responsables rindan cuentas de sus actos*".[29]

viii) Ausencia de supervisión independiente eficaz y de transparencia en los organismos de inteligencia

56. En cualquier estado democrático, la supervisión de los actos de seguridad legales debe ser una combinación de control ejecutivo, supervisión parlamentaria, revisión judicial y monitoreo por parte de autoridades expertas.

57. Ninguno de estos mecanismos funciona de manera satisfactoria en Colombia, de ahí las graves violaciones de los derechos humanos cometidas por los servicios de seguridad. Es particularmente preocupante la falta de supervisión por parte las autoridades de protección de datos y el hecho de que no se haya establecido ninguna supervisión parlamentaria.

58. Por una parte, la ley de protección de datos (art. 2 de la Ley 1581 de 2012) no aplicará a las bases de datos que contienen datos personales que "tengan como fin y contengan información de inteligencia y contrainteligencia". Por lo tanto, aunque se aplican los principios de la ley de protección de datos, no existe un regulador independiente que controle y proteja los datos personales en poder o para fines de inteligencia. En consecuencia, los siete organismos con funciones de inteligencia que existen actualmente no rinden cuentas ante el regulador de la protección de datos para los organismos públicos.

59. Esta ausencia de rendición de cuentas se ve agravada por la falta de eficacia de la comisión independiente que se creó en el Congreso para supervisar las actividades de inteligencia. Aunque la Ley de Inteligencia entró en vigencia el 17 de abril de 2013, la Comisión legal de seguimiento a las actividades de inteligencia y contrainteligencia, que es el único sistema de rendición de cuentas que beneficia a los ciudadanos, no ha podido ejecutar todas las actividades bajo su mandato debido a supuestos procedimientos de seguridad y contratación que en realidad enmascaran la falta de voluntad política. Las fallas de supervisión se hacen evidentes por la ausencia de investigaciones eficaces en varios de los casos que

[29] Observaciones finales sobre el séptimo informe periódico de Colombia (2016) CCPR/C/COL/CO/7, párr 33

han sido reportados sobre la vigilancia ilegal de las comunicaciones de políticos, periodistas y activistas de derechos humanos.

ix) Normas de retención de datos que carecen de garantías contra injerencias ilícitas en el derecho a la intimidad

60. Colombia ha impuesto a los proveedores de servicios de telecomunicaciones la obligación de retener datos para fines de investigación criminal y actividades de inteligencia.[30] Según el Consejo de Estado, la legislación colombiana establece claramente que el acceso a los datos retenidos requiere una orden judicial previa.[31]

61. Respecto a actividades de inteligencia, la Ley 1621 (2013) establece que los organismos de inteligencia pueden solicitar los datos del suscriptor, el "historial de comunicaciones" y la información de localización. La misma ley establece que los datos pueden ser retenidos por un período de cinco años. Por último, la Resolución 0912 (2008) de la Policía Nacional establece que los proveedores de servicios de telecomunicaciones deben permitir que la Policía acceda a una base de datos en la cual se debe registrar la siguiente información de los suscriptores: nombre e identificación, dirección y lugar de residencia, número de celular y fecha y estado de activación.

62. La interceptación, recolección y uso de metadatos interfiere con el derecho a la intimidad, tal como lo han reconocido expertos en derechos humanos, incluyendo el Relator Especial de la ONU sobre libertad de expresión, el Relator Especial de la ONU sobre la lucha sobre la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo y el Alto Comisionado para los Derechos Humanos. El Tribunal de Justicia de la Unión Europea señaló que los metadatos pueden permitir "extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han retenido" y concluyó que la retención de metadatos relativos a la vida privada y las comunicaciones de una persona es en sí misma, una injerencia en el derecho a la intimidad.[32] El TJUE también sostuvo en un caso diferente que el derecho de los derechos humanos prohíbe a la "legislación nacional que, con el fin de combatir el delito, prevea la retención general e indiscriminada de todos los datos de tráfico y localización".[33]

---

30 Para la investigación de delitos, el Decreto 1704 (2012) establece que la información del suscriptor y los datos de geolocalización deben ser entregados a la Fiscalía de manera inmediata cuando sea solicitada y deberán ser conservados durante cinco años. El 18 de febrero de 2016, el Consejo de Estado revisó el artículo 4 del Decreto, relacionado con la información del suscriptor y declaró la nulidad de la expresión "o demás autoridades competentes", y dejó en claro que la información del suscriptor solo puede ser solicitada por el Fiscal. Adicionalmente, el Consejo de Estado indicó que las órdenes de interceptación de comunicaciones o de retención de datos deben ser emitidas con arreglo a la Constitución y la ley.

31 Para más detalles, ver: Submission in advance of the consideration of the periodic report of Colombia, Comité de Derechos Humanos, sesión 118a, 17 de octubre - 04 de noviembre de 2016, disponible en: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fCSS%2fCOL%2f25208&Lang=en

32 Sentencia del 8 de abril de 2014, Digital Rights Ireland Ltd, C-293/12 y Kärntner Landesregierung, C-594/12, EU:C:2014:238, párrafo 27. Disponible en: http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=635772

33 Tele2 Sverige AB vs. Telestyrelsen post-Och (C-203/15); Secretary of State for the Home Department vs. Tom Watson et. al. (C-698/16), Joined Cases, Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 21 de diciembre de 2016.Concluding Observations of the Fourth Periodic Report of the

63. El Comité de Derechos Humanos, al interpretar el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, adoptó una posición similar en cuanto a que las políticas de retención de datos constituyen una injerencia en el derecho a la intimidad y que como norma general los países deberían "abstenerse de imponer la retención obligatoria de datos por terceros".[34] [35]

64. No hay un ente regulador que tenga la función de proteger los datos personales en poder de los organismos públicos ya que la Procuraduría General de la Nación, a la que la Corte Constitucional le asignó la tarea, no ha asumido esta función.

x) Prohibición de comunicaciones cifradas

65. El artículo 102 de la Ley 418 (1997) prohíbe el envío de mensajes cifrados en todos los dispositivos de comunicación que utilizan el espectro electromagnético. Sin embargo, no está claro si estas leyes también cubrirían las comunicaciones cifradas en Internet.

66. Como el Relator Especial de la ONU sobre la libertad de expresión señaló, las restricciones sobre el uso del cifrado afectan el derecho a la intimidad y la libertad de expresión, cualquier restricción de ese tipo debe ser legal, necesaria y proporcional al logro de un objetivo legítimo.[36] Dejusticia, Fundación Karisma y PI creen que la prohibición general de comunicaciones cifradas que actualmente prevé el ordenamiento colombiano no es necesaria ni proporcional.

xi) Sistema de registro de teléfonos celulares

67. Desde 2011, el gobierno colombiano ha estado desarrollando un sistema de registro de teléfonos celulares que tiene como objetivo evitar y disuadir el robo de teléfonos celulares. Un decreto del Ministerio TIC[37] estableció una medida para disminuir los incentivos de los ladrones para robar teléfonos celulares y así disminuir el robo y los delitos relacionados. Con posterioridad al decreto de expidieron una ley y regulaciones formuladas por el Regulador de Telecomunicaciones, que incluían un registro que consta de:

[34] Observaciones finales sobre el cuarto informe periódico de los Estados Unidos de América, Comité de Derechos Humanos, UN Doc. CCPR/C/USA/CO/4, párr. 22 (23 de abril de 2014)

[35] El Comité también ha señalado que los Estados Miembros deberían revisar sus regímenes de retención de datos con miras a garantizar: "que esas actividades se ajusten a sus obligaciones en virtud del artículo 17, en particular a los principios de legalidad, proporcionalidad y necesidad; [y que existan] rigurosos sistemas de supervisión independiente de la vigilancia [...] en particular velando por que el poder judicial participe en la autorización de esas medidas en todos los casos y ofreciendo a las personas afectadas recursos efectivos en caso de abuso, entre otros, cuando sea posible, una notificación a posteriori de que fueron objeto de [estas] medidas". Ver: Observaciones finales sobre el sexto informe periódico de Italia, Comité de Derechos Humanos, UN Doc. CCPR/C/ITA/CO/6, párr. 37 (28 de marzo de 2017). Ver también: Observaciones finales sobre el séptimo informe periódico del Reino Unido de Gran Bretaña e Irlanda del Norte, Comité de Derechos Humanos, UN Doc. CCPR/C/GBR/CO/7, párr. 24 (17 de agosto de 2015); Observaciones finales sobre el informe inicial de Sudáfrica, Comité de Derechos Humanos, UN Doc. CCPR/C/ZAF/CO/1, párrs. 42-43 (27 de abril de 2016).

[36] A/HRC/29/32

[37] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, Decreto 1630 de 2011 "por medio del cual se adoptan medidas para restringir la operación de equipos terminales hurtados que son utilizados para la prestación de servicios de telecomunicaciones móviles"

a. listas de números IMEI (del inglés International Mobile Equipment Identity) o bases de datos, como los llaman los documentos jurídicos, y
b. un procedimiento de verificación

68. El propósito del registro es que cada dispositivo solamente puede operar en las redes móviles si figura en una "base de datos positiva". Cuando se roba o pierde un teléfono celular, su IMEI se registra en la "base de datos negativa". Los operadores de telefonía móvil deben bloquear cualquier IMEI registrado en esta base de datos negativa para evitar que pueda utilizar sus redes. Además, se diseñó un procedimiento de verificación para que las dos bases de datos se mantengan operativas y efectivas. Con base en los metadatos de las comunicaciones, la actividad de cada teléfono celular en las redes colombianas es monitoreada con el fin de detectar los números IMEI falsificados o duplicados y los dispositivos que carecen de un certificado de conformidad.

69. Un análisis profundo de la política y los aspectos técnicos de este registro que desarrolló la Fundación Karisma encontró varios problemas desde la perspectiva de los derechos humanos.[38]

70. En primer lugar, cada IMEI está atado a la identidad de una persona ya que el registro exige que los operadores registren el IMEI, el IMSI y el número de teléfono junto con el nombre, el número de identificación y la dirección del propietario. Los requisitos obligatorios de registrar datos personales de identificación han sido criticados por el Relator Especial de ONU sobre la promoción y protección del derecho a la libertad de opinión y expresión porque eliminan la posibilidad de comunicarse anónimamente. Esto permite rastrear a las personas y facilita la vigilancia de las comunicaciones.[39]

71. En segundo lugar, el procedimiento de verificación se basa en los metadatos de las comunicaciones, que se recopilan y procesan omitiendo la protección constitucional que cobija al contenido de las comunicaciones a pesar de la injerencia en la intimidad mencionada anteriormente. Como señalamos en la sección ix) sobre retención de datos, la retención general e indiscriminada de todos los datos de tráfico y localización es contraria al derecho internacional de los derechos humanos.

72. Finalmente, el sistema afecta de manera desproporcional los derechos humanos y no es necesario. El mismo objetivo de evitar el robo de teléfonos celulares se puede lograr sin registrar los datos de identificación de las personas ni usar metadatos. Compartir la lista "negativa" de los teléfonos celulares presuntamente robados puede ser igual de efectivo y menos invasivo que el registro actual. Además, solo usar la lista "negativa" de los IMEI es la manera en que por lo general funciona en otros países y es la forma en que la GSM Association, una organización comercial que representa los intereses de los operadores de redes

[38] Castañeda, JD, Un rastreador en tu bolsillo, Fundación Karisma, julio de 2017. Disponible en: https://karisma.org.co/descargar/informe-investigacion-un-rastreador-en-tu-bolsillo/. Un resumen en inglés está disponible en: https://karisma.org.co/descargar/a-tracker-in-your-pocket-executive-summary/

[39] A/HRC/29/32, párr. 51

móviles en todo el mundo, promueve el uso del sistema.

xii) Falta de acceso a los archivos de inteligencia relevantes para la implementación del Acuerdo de Paz

73. Según el Acuerdo de Paz, en la implementación del mismo el acceso a la información en poder del Gobierno se otorgará "conforme a las normas vigentes en el momento de implementarse el Acuerdo". Las leyes actualmente aplicables que regulan el acceso a la información de inteligencia y contrainteligencia no permiten que ni la Comisión de la Verdad ni la Unidad de Búsqueda de Personas Desaparecidas tengan acceso a los archivos que sean relevantes para sus investigaciones.[40] El acceso a dicha información es extremadamente importante para estas autoridades a fin de poder determinar las violaciones de los derechos humanos cometidas durante el conflicto armado, incluyendo el uso de métodos ilícitos de vigilancia o tratamiento ilegal de datos personales por parte de los organismos de inteligencia.

74. En 2013, la Ley de Inteligencia y Contrainteligencia (Ley Estatutaria No. 1621 de 2013) creó una comisión de autoridades privadas y públicas para formular criterios de depuración de los archivos de inteligencia. Se señaló que la Comisión debería tener en cuenta diferentes factores, incluyendo los derechos fundamentales de los ciudadanos.[41] Si bien el proceso se llevó a cabo y se finalizó un conjunto de criterios, el gobierno colombiano y el presidente de la Comisión de Depuración no los hicieron públicos, alegando la confidencialidad. Si el público carece de acceso a estos criterios, se obstaculiza la capacidad de evaluar si el tratamiento de datos personales por parte de los organismos de inteligencia se realizó con arreglo a la ley o no y, en caso de tratamiento ilegal, si sus acciones se han corregido y si los ciudadanos han sido indemnizados.

xiii) Protección de bases de datos sensibles relacionadas con el Acuerdo de Paz

75. El punto 2.2.1 del Acuerdo de Paz prevé la creación de un registro de todas las organizaciones y movimientos sociales formales e informales como un instrumento que permita que las autoridades evalúen sus capacidades y respondan a sus necesidades mientras desempeñan sus funciones en el proceso de paz.[42] Este registro implica la recopilación de datos personales confidenciales, que pueden revelar, por ejemplo, el origen racial o étnico de las personas, su orientación política o su pertenencia a organizaciones sociales. Nos preocupa la centralización de estos datos y el riesgo que surge cuando no se adoptan las salvaguardas necesarias para garantizar la seguridad de los datos y la infraestructura. El uso e intercambio y el abuso ilegal de este tipo de datos, que

[40] Ver: Ramírez, A.M., Ángel, M.P., Albarracín, M., Uprimny, R. y Newman, V. (2017). Acceso a los archivos de inteligencia y contrainteligencia en el marco del posacuerdo. Bogotá: Dejusticia. Disponible en: https://www.dejusticia.org/wp-content/uploads/2017/04/fi_name_recurso_699.pdf

[41] Artículo 30 de la Ley Estatutaria 1621 de 2013 "por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones".

[42] Gobierno Nacional de Colombia y Fuerzas Armadas Revolucionarias de Colombia-Ejército del Pueblo (FARC-EP). (2016). Acuerdo final para la terminación del conflicto y la construcción de una paz estable y duradera". Disponible en: http://www.altocomisionadoparalapaz.gov.co/herramientas/Paginas/Todo-lo-que-necesita-saber-sobre-el-proceso-de-paz.aspx

se consideran datos personales sensibles en Colombia,[43] pueden conducir a la discriminación o incluso poner en peligro la vida o la seguridad personal de las personas afectadas.

76. Nuestra preocupación es apoyada por evidencia de casos anteriores en los que se accedió de manera ilegal a datos personales sensible administrados por el Estado en relación con el proceso de paz y el proceso de reparación. Por ejemplo, en 2014 se reveló que una red de personas logró acceder ilegalmente a la base de datos administrada por la Unidad para la Atención y Reparación Integral a las Víctimas.[44] Se reportó que estas personas lograron acceder a la base de datos utilizando códigos de autorización que les habían sido filtrados. Estos datos se vendieron para permitir que personas inescrupulosas se hicieran pasar por víctimas verdaderas, para acelerar el pago de la indemnización a ciertos solicitantes, o para conocer los datos personales de los denunciantes, entre otros delitos.

77. Nos preocupa la posibilidad de que ocurra un acceso ilegal similar en el registro de organizaciones y movimientos sociales. Por lo tanto, si el gobierno avanzara con la creación de este registro, debe garantizar que cumpla con los más altos estándares de protección de datos para garantizar la protección de los datos y la seguridad de su infraestructura.

VII. Recomendaciones

78. Con base en estas observaciones, Dejusticia, la Fundación Karisma y Privacy International proponen que se hagan las siguientes recomendaciones al gobierno colombiano:

- Revisar el marco jurídico que rige la vigilancia en Colombia, especialmente la Ley de Inteligencia y el Código de Policía, para garantizar que cumplan con el Pacto Internacional de Derechos Civiles y Políticos, incluyendo el artículo 17 a fin de garantizar que cualquier injerencia en el derecho a la intimidad sea necesaria y proporcional al objetivo perseguido;
- Asegurarse de que todas las actividades de interceptación, incluyendo, entre otras, el monitoreo del espectro electromagnético, solo se realicen de maneras que cumplan los principios de legalidad, necesidad y proporcionalidad;
- Modificar las normas sobre la retención de datos para garantizar que no impongan obligaciones indiscriminadas de retener los datos de las comunicaciones, y disponer que cualquier solicitud de acceso a dichos datos esté sujeta a los principios de necesidad y proporcionalidad y haya sido autorizada por los organismos judiciales.

[43] Ver: Artículo 5°, Ley Estatutaria 1581 de 2012.

[44] El Colombiano. “Siete capturados por supuesta venta de información de víctimas del conflicto”, 05 August, 2014. Available at: http://www.elcolombiano.com/historico/siete_personas_capturadas_por_supuesta_venta_de_informacion_de_las_victimas_del_conflicto-OGEC_305487

- Llevar a cabo investigaciones prontas e independientes de los informes fidedignos sobre la vigilancia ilegal de abogados, periodistas, activistas de derechos humanos y otros, con el fin de llevar ante la justicia a los perpetradores y efectuar reparaciones. Publicar los resultados de estas investigaciones;
- Reforzar la supervisión efectiva de las prácticas de vigilancia de los servicios de inteligencia y de orden público, incluyendo mediante la garantía de que la Comisión de Inteligencia y Actividades de Contrainteligencia tenga la capacidad de cumplir en su totalidad su mandato de supervisión;
- Garantizar que los procedimientos policiales del nuevo Código de Policía respeten plenamente el derecho a la intimidad;
- Divulgar qué tipo de tecnologías de vigilancia emplean los organismos colombianos de orden público y de inteligencia, cómo se regula y supervisa su adquisición y uso, y cómo están cumpliendo ley y la Constitución;
- Fortalecer las garantías efectivas relacionadas con la obtención y el tratamiento de bases de datos sensibles relacionadas con el Acuerdo de Paz;
- Revelar las políticas y los procedimientos para la manipulación de datos de los organismos de orden público y de inteligencia, a fin de garantizar que su contenido no viole los derechos humanos y cuente con la supervisión adecuada.
- Asegurar el acceso a los expedientes que contienen información de inteligencia sobre las violaciones de los derechos humanos, así como a la información de inteligencia que contribuya a la realización de los derechos a la justicia, la verdad y la reparación en la implementación del Acuerdo de Paz.