Honorables Magistrados
Corte Constitucional
E. S. D.

Expediente: D-11902

Ref: Intervención ciudadana frente a la demanda de inconstitucionalidad formulada por César Rodríguez Garavito, Vivian Newman Pont, Mauricio Albarracín Caballero, Mariluz Barragán González y María Paula Ángel Arango, contra los artículos 53, 54, 55, 56 y 57 de la Ley 1801 de 2016.

Respetados Magistrados:

Miguel Ángel Osorio Ágredo, ciudadano colombiano, con Cédula de Ciudadanía n° 76.328.811 de Popayán, domiciliado en la ciudad de Bogotá, en ejercicio de los derechos consagrados en el artículo 95, numeral 7º, de la Constitución Política de Colombia, me permito allegar a este Despacho, dentro del asunto de la referencia, en nombre de la organización Privacy International, el presente escrito de intervención ciudadana.

Esta es una traducción informal, no oficial, del escrito de intervención ciudadana redactada originalmente en inglés por Privacy International. En caso de que exista alguna duda acerca del contenido de este texto, ha de preferirse la versión en inglés[1].

INTRODUCCIÓN

1. Privacy International es una organización benéfica, de Inglaterra, fundada en 1990, dedicada a la defensa del derecho a la intimidad a nivel internacional. Su trabajo se enfoca particularmente en combatir el uso ilegal de la vigilancia. Ha litigado o intervenido en casos relacionados con el derecho a la intimidad en diferentes tribunales del mundo, incluidos tribunales de Estados Unidos, Inglaterra y Europa, tales como el Tribunal Europeo de Derechos Humanos y el Tribunal de Justicia de la Unión Europea.
2. Privacy International tiene como objetivos principales crear mayor conciencia acerca de las amenazas al derecho a la intimidad, hacer seguimiento sobre

[1] Traducido por Laura Peñaranda Currie y Miguel Ángel Osorio.

métodos y tácticas de vigilancia e informar al respecto, trabajar a nivel nacional e internacional en asegurar una fuerte protección a la intimidad y buscar formas de proteger la intimidad mediante el uso de la tecnología.

3. Privacy International se ha interesado en la acción de inconstitucionalidad interpuesta por Dejusticia contra Ley 1801 de 2016 ("Código de Policía"), dados los riesgos que esta norma supone para el derecho a la intimidad, ya que restringe la privacidad de las personas (artículos 32, 139 y 237); otorga facultades de retención de datos (artículo 95 y artículo 237) y amplía el uso de cámaras de vigilancia (artículo 146). Esto en el contexto de un marco jurídico que no ofrece salvaguardias suficientes a los derechos.
4. Esta intervención no proporciona una visión general de todas las normas internacionales que son relevantes para el caso ante esta Corte. Por el contrario, se centra en las normas europeas e internacionales de derechos humanos que Privacy International considera aplicables a las cuestiones centrales del caso, y busca en esta intervención prestar asistencia a la Corte explicando un contexto más amplio y enfatizando la trascendencia de las interferencias al derecho de intimidad.

El alcance del derecho a la vida privada

5. El artículo 32 de la Ley 1801 de 2016 (Código Nacional de Policía y Convivencia) establece una definición de "privacidad", a los efectos del Código. El derecho a la intimidad resulta condicionado, según esta definición, a que las personas se encuentren ubicadas en un área que les sea exclusiva y que se sea considerada "privada". Además, excluye de la definición de "lugar privado", y por lo tanto de la definición de privacidad, a los llamados "espacios" y "sitios" públicos.
6. El artículo 139 del Código de Policía clasifica el espacio electromagnético como un espacio público. Así, leído en conjunto con el Artículo 32, el espectro electromagnético no está cobijado por la la definición de privacidad.
7. El artículo 237 establece que los datos captados y/o almacenados por sistemas de video ubicados en espacios públicos son considerados como "públicos". Leído el artículo 237 en conjunto con el artículo 32, estos datos tampoco quedarían amparados por la definición de privacidad.
8. En el Informe Alternativo previo a la consideración del informe periódico presentado por Colombia ante el Comité de Derechos Humanos, 118.ª reunión, 17 de octubre - 04 de noviembre de 2016, Privacy International[2] señaló:

> "*El artículo 32 contiene una definición de privacidad demasiado restringida. Al definir el derecho a la privacidad 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*

[2] http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/COL/INT_CCPR_CSS_COL_25208_E.pdf

privacidad con el derecho al libre desarrollo de la personalidad y con el derecho a la inviolabilidad del hogar. Por lo tanto, al vincular el derecho de privacidad con la existencia de espacios privados, se excluye de protección a las personas o bienes (tales como automóviles o dispositivos electrónicos) ubicados en lugares públicos, incluyendo bares, restaurantes, etc.

Por el contrario, el artículo 139 define el espacio público de una manera muy amplia, incluyendo en esta definición, en particular, a "el espectro electromagnético".

El resultado de estas definiciones resulta preocupante respecto de la protección de la intimidad, particularmente cuando se considera que el artículo 237 establece que: "(i) la información, imágenes, y datos de cualquier índole captados y/o almacenados por los sistemas de video o los medios tecnológicos que estén ubicados en el espacio público, o en lugares abiertos al público, serán considerados como públicos y de libre acceso; y (ii) los sistemas de video y medios tecnológicos, de propiedad privada o pública, que se encuentren instalados en espacios públicos, áreas comunes, lugares abiertos al público o que siendo privados trascienden a lo público, se vinculará de manera permanente o temporal a la red que para tal efecto disponga la Policía Nacional". Así, estas disposiciones podrían incluso significar que las comunicaciones que viajan a través del espectro electromagnético estarían excluidas de la protección de la privacidad".

9. El derecho a la intimidad se encuentra establecido en términos amplios por:

a. El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP), el cual prevé el derecho que tiene toda persona a ser protegida contra las injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, al igual que contra ataques ilegales a su honor o reputación. Cualquier interferencia con el derecho a la intimidad sólo puede justificarse si está de acuerdo con la ley, si tiene un objetivo legítimo y si se lleva a cabo de una manera que sea *necesaria* y *proporcionada*. Las actividades de vigilancia sólo deben adelantarse cuando son el único medio para alcanzar un objetivo legítimo o cuando, existiendo múltiples medios, son las que cuentan con menos

probabilidades de vulnerar los derechos humanos[3].

b. El artículo 11 de la Convención Americana sobre Derechos Humanos establece:

1. "Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad."

2. "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."

3. "Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

10. El derecho a la intimidad implica la importancia del derecho a la dignidad humana y a la autonomía personal, así como a la interacción que una persona tiene con los demás, tanto en privado como en público. El derecho a la intimidad no puede depender de si una persona se encuentra en un lugar público o privado. Rige tanto en uno como en otro e incluso en contextos diversos como lo es el uso del espectro electromagnético[4].

---

[3]Human Rights Committee, General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17); see also Report by the UN High Commissioner for Human Rights, the right to privacy in the digital age, A/HRC/27/37, 30 June 2014. See also International Principles on the Application of Human Rights to Communications Surveillance, available at https://necessaryandproportionate.org.

[4]Privacy International raised the reference to 'monitoring the electromagnetic spectrum' in submission to the Human Rights Committee 116th Session, March 2016. https://www.privacyinternational.org/sites/default/files/HRC_colombia.pdf §2

Monitoring of electromagnetic spectrum constitutes an interference with the privacy of communications. It was noted in those submissions that 'Monitoring' the electromagnetic spectrum is not defined in the law (nor in the Colombian constitution).

Further, monitoring the electromagnetic spectrum could include filtering, analysing and monitoring emails, text messages and phone calls that carried upon the electromagnetic spectrum. Those acts constitute 'interception' of the communication and thereby interfere with the privacy of the person sending and receiving the information. 'Monitoring' the electromagnetic spectrum, thus, intrinsically involves an interference with the right to privacy.

Even if one contends that the means of 'monitoring' the electromagnetic spectrum without violating the privacy of communications exist, they pertain to an extremely narrow set of activities such as heat detection tools and direction-finding tools and antenna. All other forms of 'monitoring' the electro magnetic spectrum necessitate an interference with communication of a type that means that it is not possible to conclude anything other than that the monitoring has resulted in the

11. El Comité de Derechos Humanos, en sus observaciones finales sobre Colombia[5], expresó su preocupación ante el hecho de que:

> *"32…el nuevo Código de Policía, que entrará en vigor enero de 2017, 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)".*
>
> *"El Estado parte debe:*
>
> *(...) d) Velar por que la aplicación de la legislación que regule cuestiones que puedan tener consecuencias en el goce del derecho a la vida privada, en particular la Ley 1621 y el nuevo Código de Policía, sea totalmente conforme con las obligaciones que surgen del Pacto, en particular el artículo 17."*

12. Privacy International comparte las preocupaciones del Comité de Derechos Humanos según las cuales la definición estrecha de "privacidad" establecida por el Código de Policía no es compatible con la manera como internacionalmente se entiende este derecho.

En el Informe Alternativo previo a la consideración del informe periódico presentado por Colombia ante el Comité de Derechos Humanos, 118.ª reunión, 17 de octubre - 04 de noviembre de 2016, Privacy International[6] expresó *preocupación por las prácticas de vigilancia por parte de las agencias de inteligencia y de orden público*:

> *"La legislación nacional que rige la vigilancia es inadecuada, poco clara en cuanto a las competencias, el alcance y la capacidad de vigilancia por parte del Estado, por lo que no cumple las normas de derechos humanos exigidas para proteger a las personas de interferencias ilegales al derecho a la intimidad".*

---

communication being intercepted.

[5] http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR/C/COL/CO/7&Lang=en

[6] http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/COL/INT_CCPR_CSS_COL_25208_E.pdf

13. En el Informe Alternativo se planteó además la preocupación por el alcance de la vigilancia de la ley 1621 de 2013 (Ley de Inteligencia) en la que se regulan las actividades de inteligencia y contrainteligencia, incluida la "vigilancia del espectro electromagnético", aspecto central del Código de Policía.

> *"Las organizaciones reiteran su preocupación por el alcance de la vigilancia bajo la Ley de Inteligencia (Ley Nº 1621 de 2013) en la cual se regulan las actividades de inteligencia y contra-inteligencia, incluida la "monitoreo del espectro electromagnético.*
>
> *Las respuestas escritas presentadas por el Gobierno colombiano sobre este punto (párrafos 95 a 96) se limitan a describir el alcance de la ley y la sentencia de la Corte Constitucional, sin abordar el tema del alcance del monitoreo del espectro electromagnético ni definir esta actividad.*
>
> *Para resumir las preocupaciones de las organizaciones:*
>
> - *Los propósitos para los cuales se puede obtener información (artículo 4) son excesivamente amplios, especialmente aquellos relacionados con garantizar la seguridad nacional, la soberanía, la integridad territorial, la seguridad y la defensa de la nación, la protección de las instituciones democráticas y los derechos de los residentes y ciudadanos colombianos, así como la protección de los recursos naturales e intereses económicos de la nación[7];*
>
> - *El "monitoreo" del espectro electromagnético no está definido en la ley (ni en la Constitución colombiana). Sin ninguna definición, el "monitoreo" del espectro electromagnético podría incluir el filtrado, el análisis y el monitoreo de correos electrónicos, mensajes de texto y llamadas telefónicas que se realizan a través del espectro electromagnético. Estos actos constituyen "interceptación" de las comunicaciones y por lo tanto interfieren con la privacidad de la persona que envía y recibe la información;[8]*

[7]UN Doc. CCPR/C/COL/Q/7, 26 April 2016.

[8]Privacy International, 'Shadow State: Surveillance, Law and Order in Colombia', September 2015, p. 33, available at: https://privacyinternational.org/node/635.

- *De hecho, el gobierno acepta (en el párrafo 95) que este "monitoreo" puede incluir información que no es útil para el cumnecesaria a efectos de inteligencia, pero no reconoce que, como resultado, tal "monitoreo" constituya una injerencia en la privacidad del individuo, la cual debe someterse a la misma prueba estricta de legalidad, necesidad y proporcionalidad;*
- *La Ley de Inteligencia del 2013 se limita a exigir que los directores de las agencias de seguridad competentes autoricen el "monitoreo" del espectro electromagnético".*

14. El Tribunal Europeo de Derechos Humanos (TEDH) ha desarrollado una importante jurisprudencia sobre el alcance del derecho a la privacidad en virtud del artículo 8 del Convenio Europeo de Derechos Humanos, cuya formulación es similar al artículo 11 de la Convención Interamericana. Esta jurisprudencia es particularmente pertinente en este caso porque demuestra que el derecho a la privacidad puede estar implicado incluso en lugares públicos.

15. El artículo 8 del Convenio Europeo de Derechos Humanos ("CEDH") establece:

> *"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*
>
> *2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".*

16. El Tribunal Europeo de Derechos Humanos, al aplicar el artículo 8 del CEDH en el asunto *Von Hannover c. Alemania* (solicitud nº 59320/00), de 24 de junio de 2004, relativo a las fotos del solicitante tomadas exclusivamente en lugares públicos[9], decidió:

> *"50. La Corte reitera que el concepto de vida privada se extiende a aspectos relacionados con la identidad personal, como el nombre de una persona o el retrato de una persona.*

[9] §19

Además, la vida privada, según la Corte, incluye la integridad física y psicológica de una persona; la garantía otorgada por el artículo 8 de la Convención tiene por objeto primordial garantizar, sin injerencias externas, el desarrollo de la personalidad de cada individuo en sus relaciones con otros seres humanos. Por lo tanto, incluso en el contexto público existe una zona de interacción de una persona con otra que puede caer dentro del ámbito de la "vida privada".

51. La Corte también ha indicado que, en determinadas circunstancias, una persona tiene una "expectativa legítima" de protección y respeto de su vida privada. Así, a propósito de cierto caso relativo a la interceptación de llamadas telefónicas en los establecimientos comerciales, ha declarado que la demandante "habría tenido una expectativa razonable de privacidad para tales llamadas" (véase la sentencia Halford contra Reino Unido de 25 de junio de 1997)".

17. De manera similar, en P.G. Y J.H. V El Reino Unido (Solicitud nº44787 / 98) 25 de septiembre de 2001, el TEDH declaró:

"56. La vida privada es un término amplio que no es susceptible de definición exhaustiva. Esta Corte ya ha sostenido que la identificación de género, el nombre y la orientación sexual, así como la vida sexual, son elementos importantes de la esfera personal protegida por el artículo 8. El artículo 8 también protege el derecho a la identidad y el desarrollo personal, así como el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior. Puede incluir actividades de carácter profesional o empresarial. Por lo tanto, existe una zona de interacción de una persona con otra, incluso en un contexto público, que puede caer dentro del ámbito de la "vida privada".

57. Son varios los elementos que resultan relevantes para evaluar si la vida privada de una persona se ve afectada por medidas adoptadas fuera del hogar o de espacios privados".

18. La decisión señala además que:

"Consideraciones con respecto a la vida privada pueden surgir, sin embargo, cuando cualquier registro sistemático o permanente se materialice del ámbito público".

19. El acelerado desarrollo del ámbito de datos creados por las nuevas tecnologías permite el rastreo a gran-escala de personas en lugares públicos de manera que representa una infracción altamente intrusiva en la privacidad. Las técnicas utilizadas incluyen el uso de la tecnología de reconocimiento facial; *body-worn video* (uso de cámaras portables llevadas

en el cuerpo); tecnología automatizada de reconocimiento de placas de vehículos; vigilancia de redes sociales; y el uso de vehículos aéreos no tripulados (drones). Los datos reunidos pueden revelar la ubicación, las opiniones personales, así como información sobre las preferencias de una persona, su sexualidad y el estado de salud.

20. Las preocupaciones surgidas a raíz de dicho monitoreo se han planteado en los Tribunales Supremos de los Estados Unidos y del Reino Unido. En *United States v Jones*, 132 S Ct 945 (2012), un caso de la Corte Suprema de los Estados Unidos que abordó el monitoreo de movimientos principalmente públicos por la tecnología del GPS, la Jueza Sotomayor explicó en su opinión final, en 956:

> *"Tener conciencia de que el Estado puede estar vigilando, va en detrimento de las libertades de asociación y expresión. Y el poder irrestricto del Estado para reunir datos que revelan aspectos de carácter privado de la identidad es puede dar lugar a abusos* ".

21. Estos temas fueron abarcados por Lord Toulson de la Corte Suprema del Reino Unido en su voto disidente en R *(Catt) v Comisionado de Policía de la Metrópolis & Anor* [2015] UKSC 9, en la sección 69:

> "*Uno podría preguntarse por qué importa esto, si no existe riesgo de que la policía divulgue indebidamente la información a otros. Es importante porque en la sociedad moderna el Estado tiene poderes muy amplios para llevar registros de sus ciudadanos. Si las actividades de un ciudadano son lícitas, deben estar libres de seguimiento por parte del Estado a menos que tal seguimiento sea realmente necesario por razones de interés público y, en dicho caso, procederá solamente durante el tiempo necesario*"

<u>Recaudo, retención y acceso a los datos personales</u>

22. El artículo 95 del Código de Policía establece la obligación de registrar el IMEI (Identificador Internacional de Equipo Móvil), un número que identifica exclusivamente un teléfono móvil[10], junto con el nombre, apellido, dirección y número de teléfono de contacto.

23. El Tribunal de Justicia de la Unión Europea ("TJUE"), en la Sentencia en los asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland y Seitlinger y Otros*, sentencia de 8

[10] As noted in C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014 §16 '(d) data necessary to identify users' communication equipment or what purports to be their equipment' includes '(2) (iii) the International Mobile Equipment Identity (IMEI) of the calling party … (v) the IMEI of the called party'

de abril 2014, sostuvo que el recaudo, retención y el uso de los metadatos/datos de comunicación interfiere con el derecho a la privacidad. Estos datos constituyen datos personales. Su retención y recaudo obligatorios por parte de las autoridades plantea preocupaciones importantes, dado que estos datos pueden ser utilizados para elaborar perfiles de personas, dando lugar de este modo a una mayor vulneración de su intimidad. La retención de datos del IMEI, tal como lo requiere el artículo 95, puede constituir uno de los elementos principales que permitan la elaboración de dicho perfil.

24. En el Informe Alternativo previo a la consideración del informe periódico presentado por Colombia ante el Comité de Derechos Humanos, 118.ª reunión, 17 de octubre - 04 de noviembre de 2016, Privacy International[11] señaló respecto a las cuestiones de los datos de los suscriptores:

> *"Tratándose de investigaciones criminales, el Decreto 1704 de 2012 establece que tanto la información de los suscriptores[12], como su información de ubicación[13], debe ser conservada por cinco años"*
>
> *...*
>
> *"Además, el Ministerio de Tecnologías de la Información y las Comunicaciones ha puesto en marcha una estrategia para contrarrestar el robo de teléfonos celulares, la cual implica la creación de una base de datos que asocia el número IMEI con la SIM card, y con información personal del usuario tal como número de identificación, nombre y dirección. Los proveedores deben comprobar el ID de usuario mediante varias fuentes, tales como la Registraduría Nacional del Estado Civil y centrales de riesgo crediticio.*
>
> *Las autoridades administrativas, policiales y judiciales pueden acceder a esta información. Además, no existe norma que precise cuáles son las razones que deben presentar las autoridades para acceder a las bases de datos. Tampoco existe supervisión del acceso de las autoridades a la base de datos, facilitando así la comisión de abusos y aumentando el riesgo para las violaciones de privacidad".*

[11] http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/COL/INT_CCPR_CSS_COL_25208_E.pdf

[12] Article 4 of Decree 1704 of 2012.

[13] Article 5 of Decree 1704 of 2012.

25. Además del Tribunal de Justicia de la Unión Europea (TJUE), varios organismos internacionales han expresado serias preocupaciones por la retención indiscriminada de datos. Por ejemplo, según el Informe del *Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, U.N. Doc. A/HRC/29/32 (22 de mayo de 2015):

> *"55. Las políticas amplias de retención obligatoria de datos limitan la capacidad de los usuarios para conservar el anonimato. La capacidad de un Estado para exigir a los proveedores de servicios de telecomunicaciones y de Internet que recopilen y almacenen información sobre las actividades en línea de todos los usuarios ha resultado de forma inevitable en que el Estado tenga la huella digital de todos los usuarios. La capacidad del Estado para recopilar y almacenar datos personales amplía su capacidad para llevar a cabo labores de vigilancia e incrementa la probabilidad de que se robe y difunda la información personal".*

26. El Comité de Derechos Humanos de la ONU, en sus Observaciones Finales Sobre el Informe Inicial de Sudáfrica, el Comité de Derechos Humanos, U.N. Doc. CCPR/C/ZAF/CO/1 (27 de abril de 2016), observó:

> *"42. [El Comité] también está preocupado por el amplio alcance de la retención de datos previsto en el [Regulación del 2002 Sobre Intercepción de Comunicaciones y Provisión de Información relacionada con la Comunicación...*
>
> *43. El Estado Parte debería ... considerar revocar o limitar el requisito de retención obligatoria de datos por terceros ... "*

27. El Alto Comisionado de las Naciones Unidas para los Derechos Humanos ha dicho, en un informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, que el derecho a la intimidad en la era digital, U.N. Doc. A /HRC /27/37 (30 de junio de 2014):

> *"26. La preocupación sobre si el acceso a los datos y su uso se ajustan a objetivos legítimos específicos plantea también dudas sobre la creciente colaboración de los gobiernos con entidades del sector privado para que conserven datos "por si acaso" los necesita el gobierno. La conservación obligatoria de datos de terceros —característica frecuente de los regímenes de vigilancia de muchos Estados, cuyos gobiernos exigen a las compañías telefónicas y a los proveedores de servicios de Internet que almacenen los metadatos acerca de las comunicaciones y la ubicación de sus clientes para que las fuerzas del orden y los organismos de inteligencia puedan acceder posteriormente a ellos— no parece necesaria ni proporcionada"*

28. También el Tribunal de Justicia de la Unión Europea (TJUE) ha vuelto recientemente a

abordar la cuestión de la retención de datos en los asuntos acumulados C-203/15 y C-696/15 *Tele2 Sverige and Watson* ECLI:EU:C:2016:970 (‘***Watson***’). El Tribunal sostuvo:

> *"1. El artículo 15(1), de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, en relación con los artículos 7, 8, 11 y 52(1), de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que se opone a una normativa nacional que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica.*
>
> *2. El artículo 15(1), de la Directiva 2002/58, en su versión modificada por la Directiva 2009/136, en relación con los artículos 7, 8, 11 y 52(1), de la Carta de los Derechos Fundamentales, debe interpretarse en el sentido de que se opone a una normativa nacional que regula la protección y la seguridad de los datos de tráfico y de localización, en particular el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar dicho acceso, en el marco de la lucha contra la delincuencia, a los casos de delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, y sin exigir que los datos de que se trata se conserven en el territorio de la Unión ".*

29. Teniendo en cuenta la naturaleza invasiva de la retención de datos de los suscriptores, la sentencia subraya que la combinación de dichos datos con otros ya obtenidos por las autoridades puede dar como resultado la construcción de el perfil completo de una persona, interfiriendo así significativamente en la privacidad. Los datos de los suscriptores pueden ser utilizados para asociar una persona con cierta conversación, ubicación y horario. Para ello, basta con que el Gobierno correlacione el nombre de una persona, un número telefónico y otros datos de comunicaciones previamente recopilados:

> *"98. Así, los datos que deben conservar los proveedores de servicios de comunicaciones electrónicas permiten rastrear e identificar el origen de una comunicación y su destino, determinar la fecha, la hora, la duración y la naturaleza de una comunicación así como el equipo de comunicación de los usuarios, y localizar el equipo de comunicación móvil. Entre esos datos se encuentra el nombre y la dirección del abonado o usuario registrado, los números de teléfono de origen y destino y una dirección IP para los servicios de Internet. Estos datos permiten, en concreto, saber con qué persona se ha comunicado un abonado o un usuario registrado y de qué modo, así como determinar el momento de la comunicación y el lugar desde el que se ha realizado. Además, permiten conocer la frecuencia de las comunicaciones del abonado o del usuario registrado con determinadas personas durante un*

período concreto".

"99. Estos datos, considerados en su conjunto, permiten extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los círculos sociales que frecuentan (...). En particular, estos datos proporcionan medios para determinar(...) el perfil de las personas afectadas, información tan sensible, a la luz del respeto de la vida privada, como el propio contenido de las comunicaciones.".

30. En su sentencia, la CJEU estableció orientaciones claras e inequívocas sobre la retención de datos:

a. Dado que la retención de datos implica una grave injerencia en la intimidad, dicha retención sólo es apropiada con el propósito de descubrir y prevenir delitos graves (incluidos los delitos de terrorismo) (§115, 119).

b. Se prohíbe la retención generalizada e indiferenciada de los datos de tráfico y localización de los abonados y usuarios registrados (§112).

c. El acceso a los datos retenidos sólo podrá concederse en relación con la lucha contra la delitos y exclusivamente respecto de los datos de personas de las que se sospeche que planean, van a cometer o han cometido un delito grave o que puedan estar implicadas de un modo u otro en un delito grave (§119).

d. Debe existir un control previo de las solicitudes de acceso, ejercido por un órgano jurisdiccional o una autoridad administrativa independiente. La solicitud deberá estar motivada, excepto cuando se trate de casos de urgencia. (§ 120).

e. Deben establecerse medidas que permitan informar a las personas cuyos datos han sido retenidos, de modo tal que puedan interponer las acciones necesarias para la protección de sus derechos, siempre y cuando dicha comunicación no comprometa las investigaciones que adelantan esas autoridades. (§121).

31. Privacy International manifiesta su preocupación por el hecho de que el artículo 95 no cumple con estos estándares.

CONCLUSIÓN

32. Dado que el derecho a la intimidad se ve comprometido cuando la policía y otras autoridades recaudan datos personales y/o realizan vigilancia en lugares públicos, es necesaria la aplicación de las salvaguardias propias de la restricción de este derecho. Tanto

el marco jurídico internacional como el europeo, a los que se hace referencia en este documento, señalan los estándares que deberían ser respetados.

33. Privacy International considera que el artículo 32, el numeral 8 del artículo 95, el artículo 139, parágrafo 2 del artículo 146, y el artículo 237, en sus párrafos 1° y 2°son potencialmente incompatibles con los principios de derechos humanos internacionalmente reconocidos.

Atentamente,

Miguel Ángel Osorio Ágredo