Bogotá, 4 de marzo de 2016

Señores(as)
Relatoría Especial sobre el derecho a la privacidad
Prof. Joe Cannataci
Relator Especial

Respetado Señor Relator:

En primer lugar, las organizaciones que suscribimos la presente comunicación queremos manifestarle nuestra complacencia por la creación y puesta en funcionamiento del mandato de la Relatoría Especial sobre el derecho a la privacidad por parte del Consejo de Derechos Humanos de Naciones Unidas, así como su elección como Relator para este primer periodo. Le deseamos éxitos en su trabajo con la confianza que será la oportunidad para que a nivel global se posicione la necesidad de generar un consenso en torno a la importancia de la intimidad como valor fundamental para la garantía de los derechos humanos. En esta ocasión, las organizaciones suscritas nos dirigirnos a usted con el propósito de documentarlo brevemente sobre los principales aspectos que en Colombia determinan la garantía y el respeto del derecho a la intimidad en la era digital, pues consideramos puede ser de su interés para el ejercicio del mandato que le ha encomendado el Consejo de Derechos Humanos. Con en este propósito, hemos hallado pertinente informarle de los seis temas que consideramos de mayor relevancia y que podrían serle de utilidad para evaluar la situación de protección del derecho a la intimidad en Colombia.

1. Legislación

Como en un número importante de países, en Colombia los diferentes instrumentos, mecanismos y herramientas legales se encuentran rezagados frente a los avances cada vez más rápidos e insospechados de la tecnología. De ahí que, uno de los principales focos de afectación del derecho a la intimidad provenga de la insuficiencia o inapropiada regulación. A continuación enunciamos algunos ejemplos de ello:

Monitoreo del espectro: La legislación colombiana permite a los organismos de inteligencia vigilar las comunicaciones de las personas monitoreando el espectro electromagnético. Este tipo de recaudo de información no es considerado por la legislación como una "interceptación de las comunicaciones", ni como una injerencia arbitraria o ilegal a la intimidad, razón por la

cual esta actividad de los organismos de inteligencia no está sometida a ningún tipo de control judicial.[1]

Retención de datos: Los proveedores de servicios de telecomunicaciones están obligados a retener determinados datos para efectos de investigaciones penales. Estos datos son la identificación del usuario (identidad, dirección de facturación y tipo de conexión) y la información necesaria para ubicar geográficamente un dispositivo en tiempo real.[2] La agencias de inteligencia pueden solicitar esta misma información y, adicionalmente, pueden conocer el "historial de comunicaciones" de los abonados telefónicos.[3] Según las mismas normas, tanto para investigaciones penales como para inteligencia, los operadores deben conservar la información por cinco años. Estas normas además imponen un período de retención desproporcionado de cinco años y no obligan a las autoridades a obtener autorización judicial para solicitar los datos.[4] Tampoco se establece claramente sobre qué tipo de comunicaciones recae el deber de retención, por lo que puede expandirse, con los mismos defectos, a cualquier medio que empleen las empresas operadoras de servicios de telecomunicaciones.

Controles a las actividades de inteligencia y contrainteligencia: La legislación colombiana no prevé controles y supervisión a las actividades de inteligencia que sean específicos, independientes, externos y tengan pleno acceso a la información. Existe un órgano que ejerce un control simplemente político y que aún no ha iniciado el ejercicio de sus funciones. Se trata de la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia, conformada por 8 congresistas.[5] La ausencia de controles y supervisión específicos es causa, en gran medida, del abuso e ilegalidad en que han incurrido recientemente los organismos de inteligencia colombianos, vulnerando gravemente el derecho de las personas a la intimidad.[6]

Cifrado de comunicaciones: Desde 1993 existe una norma que ha sido prorrogada constantemente, la última vez en 2014 por otros cuatro años, y que prohíbe el envío de "mensajes en lenguaje cifrado o ininteligible".[7] Aunque las autoridades han respondido que tal prohibición no compromete el uso de cifrado en medios digitales, la misma es demasiado vaga y debe ser retirada del ordenamiento jurídico colombiano. Sin embargo y paradójicamente, la Ley de actividades de inteligencia y contrainteligencia establece que los operadores deben ofrecer un canal de comunicación que permita realizar llamadas cifradas exclusivamente para beneficio del "alto gobierno" y los agentes de inteligencia y contrainteligencia.[8]

Uso ilegítimo de herramientas de hackeo: La filtración de información de la empresa italiana Hacking Team confirmó que la Dirección Nacional de la Policía adquirió Galileo, un software de control remoto que ofrecía esta compañía y que tiene la capacidad de tomar control de los dispositivos objetivo[9]. Aunque la policía negó tener contacto con esa empresa, el software fue distribuido a través de otra empresa en Colombia. Hasta el momento no ha habido un debate público sobre la posibilidad de que las autoridades puedan atacar y tomar

control de dispositivos electrónicos para recopilar información y mucho menos existe legislación sobre el tema. Organizaciones de la sociedad civil han expresado en reiteradas ocasiones preocupación sobre la adquisición que hacen las autoridades de capacidades tecnológicas cuya legitimidad está en duda, contraviniendo deberes básicos de transparencia y participación.[10]

Bases de datos víctimas: El Estado adelanta una política de reparación integral a las víctimas del conflicto armado colombiano. Existen al menos dos grandes bases de datos fundamentales para el éxito de esta política, las cuales almacenan información personal y sensible para la seguridad de las personas: el Registro Único de Víctimas (RUV) y el Registro de Tierras Presuntamente Despojadas y Abandonadas Forzosamente. Hay razones para creer que el Gobierno no tiene una política pública específica y unificada de garantías a la privacidad de este sector de la población. La débil protección de la privacidad de las víctimas del conflicto armado constituye, además, un riesgo contra la vida las personas. Existirían casos en los cuales los perpetradores han tenido acceso a este tipo de bases de datos.[11]

Reserva absoluta de los documentos de inteligencia: En Colombia es casi imposible evaluar la legalidad de las actividades de inteligencia una vez han interferido con el derecho a la intimidad de la ciudadanía. Esto se debe a varias razones. De una parte, al extenso plazo de retención de datos a que están obligados los proveedores de servicios de telecomunicaciones. De otra, a que la Ley de Habeas Data -o protección a los datos personales- no le es aplicable a los organismos que componen la comunidad de inteligencia.[12] Además, no hay rendición de cuentas por parte de los organismos de inteligencia, pues, como se mencionó antes, la Comisión Legal de Seguimiento no ha iniciado funciones. Por último, a partir de una interpretación literal de la ley de inteligencia la comunidad de inteligencia ha asumido que los documentos, información y elementos técnicos de inteligencia están sometidos a una reserva general, automática y a futuro por un período de 30 años, un plazo excesivo cuando se compara con el término de 15 años de cualquier otra documento reservado.[13] En estas condiciones, es difícil conocer cuáles son las actividades de inteligencia y controlar cómo éstas interfieren con el derecho a la intimidad de los ciudadanos.

2. Comisión asesora de depuración de archivos de inteligencia

En Colombia existe un legado de abusos y uso ilegítimo de las actividades de inteligencia y contrainteligencia, que se hizo especialmente evidente durante la década del 2000. Una de las herramientas contempladas por la ley de inteligencia y contrainteligencia para garantizar que el almacenamiento de la información que reposa en las bases de datos de estos organismos no transgreda los fines y límites legales de este tipo de actividades, fue la creación de una Comisión Asesora para la Depuración de Datos y Archivos de Inteligencia y Contrainteligencia. Esta comisión está encargada de formular recomendaciones al Gobierno Nacional sobre los criterios de permanencia, retiro y destino de los mismos. Para ello, se le ha dado un periodo de trabajo de dos años, que vence en julio del presente año. Este proceso debería concluir con un plan estructural de depuración, dirigido a salvaguardar el derecho a la

intimidad de las personas cuya información fue arbitraria o ilegalmente recaudada, y resolver las eventuales tensiones que surjan entre la seguridad nacional y el derecho a la intimidad, de un lado, y el derecho a la verdad, a la memoria y al acceso a la información pública, de otro. A este respecto, serían muy apreciados el conocimiento y las eventuales recomendaciones del Relator.

3. Aumento de capacidad para hacer vigilancia selectiva y masiva

A pesar de los innumerables escándalos de interceptaciones ilegales de comunicaciones que conoce el país desde hace años, las autoridades siguen adquiriendo herramientas técnicas para aumentar su capacidad de interceptar teléfonos celulares, tráfico de internet y penetrar dispositivos electrónicos (ver 'Uso ilegítimo de herramientas de hackeo'). De acuerdo con investigaciones de Privacy International[14] y de medios nacionales, la policía cuenta con tres sistemas de interceptación: Esperanza, PUMA y el SIGD.

Esperanza, aunque funciona bajo autorización de la fiscalía, ha sido usada para interceptar comunicaciones de números no autorizados. Algunas de las víctimas de esas interceptaciones fueron defensores de derechos humanos que terminaron siendo desaparecidos.[15] Por su parte, el desarrollo de la Plataforma Única de Monitoreo y Análisis (PUMA) fue detenido por la Fiscalía General por falta de garantías para su uso legítimo. Sin embargo, el año pasado se reportó que PUMA estaría siendo reactivado por la Policía.[16] El Sistema Integrado de Grabación Digital (SIGD), desconocido hasta ahora por la población, está a cargo de un organismo de inteligencia de la Policía Nacional que no está autorizado a hacer interceptación de comunicaciones. El funcionamiento de estos sistemas de interceptación, especialmente de PUMA y el SIGD, no es claro y no tiene controles adecuados, pues no parecen requerir la orden de un fiscal y el control posterior de un juez para interceptar las comunicaciones de una persona. Estos sistemas se han fortalecido a la vez que han incrementado los ataques a periodistas, defensores de derechos humanos, políticos de oposición y jueces.[17] Adicionalmente, las ciudades están aumentando el número de cámaras de vigilancia, algunas de ellas con capacidad de reconocimiento facial. Por ejemplo, en la capital del país, se instalaron 1305 cámaras de las que 158 son de "ultra alta definición" y fueron instaladas en algunas vías principales, el estadio de fútbol y el parque más grandes de la ciudad. También se instalaron aproximadamente 180 cámaras en las estaciones del sistema de transporte, 24 de ellas pueden hacer reconocimiento facial y son operadas desde un centro de control independiente.[18] El incremento de cámaras es percibido como una estrategia efectiva en sí misma en contra del crimen, pero no existen reglas claras sobre qué autoridades pueden acceder a estos datos, por cuánto tiempo y para qué casos. Tampoco hay reglas sobre la eliminación de esta información. Finalmente, como estrategia para combatir el hurto de celulares, el gobierno nacional ha implementado el registro obligatorio de tarjetas SIM y la inscripción del IMEI de cada dispositivo en bases de datos con el fin de bloquear los aparatos reportados como robados o perdidos.[19] El gobierno nacional no ha analizado el impacto al derecho a la intimidad que esta medida puede comportar. Además, se suma a otras facultades que tiene la policía, como es la de tener acceso a una base de datos que deben mantener los

operadores de telefonía y donde se puede consultar los nombres e identificación, el lugar y dirección de residencia de quienes reciben el servicio, así como el número celular y su fecha y estado de activación.[20]

4. Hostigamientos a defensores y defensoras de derechos humanos y periodistas

En los últimos años, Colombia reporta índices muy altos de agresiones contra defensoras y defensores de derechos humanos, siendo la modalidad más frecuente las amenazas como medio para amedrentar y generar zozobra entre quienes se dedican a esta actividad.[21] Estas amenazas, frecuentemente, son canalizadas a través de correos electrónicos y mensajes de texto (SMS), y no cuentan con acciones específicas de las autoridades judiciales para dar con el paradero de los autores de las mismas, a pesar de contar con información sobre los servidores donde se originan los mensajes. También es cada vez motivo de mayor preocupación el robo de información sensible como modalidad de agresión contra defensores y defensoras, pues se trata de la sustracción de información relacionada con graves violaciones a los derechos humanos mediante el hurto de los equipos donde esta se aloja. Lo anterior llama la atención porque la ausencia de investigaciones judiciales serias en estos casos hacen que las herramientas provistas en la era digital —como el correo electrónico, los SMS o los hardware de almacenamiento— representen condiciones de vulnerabilidad para la defensa de los derechos humanos en Colombia.[22]

Por otro lado, la situación de hostigamientos a periodistas es una constante. A pesar del gran escándalo que significó el descubrimiento de seguimientos ilegales por parte de funcionarios del DAS, las denuncias sobre este tipo de acciones siguen existiendo. Según cifras de la Fundación para la Libertad de Prensa, tanto en 2015 como en 2014, se registraron 6 casos de agresiones contra periodistas en entornos digitales.[23] Los principales casos denunciados en esos años son, en 2014, la existencia de una sala de operaciones de inteligencia del Ejército, conocida como "Andrómeda", bajo la fachada de un café internet. Desde ahí, se hacía seguimiento a representantes del gobierno en las negociaciones de paz con las FARC. Además, se tuvo conocimiento de que en ese sitio se había interceptado correos electrónicos de periodistas y de otras personas. En 2015, la realización de seguimientos ilegales e intromisiones en computadores de periodistas que estaban realizando investigaciones relacionadas con posibles hechos de corrupción en la Policía Nacional.[24] Adicionalmente, se destaca que en la tercera encuesta nacional a periodistas, realizada por el Proyecto Antonio Nariño, se refleja que un 20% de los encuestados han percibido que agentes del Estado los han vigilado ilegalmente.[25]

5. Cultura de protección a la intimidad en la era digital

Las redes sociales y las tecnologías de la comunicación llevan a los usuarios a sobreexponer su intimidad, ya sea de forma directa o indirecta. Por eso, hay quienes dicen —como es el caso del fundador y CEO de Facebook, Mark Zuckerberg— que "la edad de la privacidad se ha acabado". A pesar de que creemos que la intimidad es un derecho fundamental y que

como tal no puede desaparecer, consideramos que en la era digital hay una ausencia de cultura de protección a la intimidad. Ausencia que es preocupante si se tiene en cuenta que el ciberespacio también está siendo utilizado para trasladar, e incluso amplificar, realidades sociales que son continuamente denunciadas y rechazadas, pero que aún persisten y se siguen multiplicando: la misoginia, el sexismo, el racismo, la homofobia, etc. A pesar de que esto está sucediendo en todo el mundo, en Colombia es especialmente peligroso, dado que se trata de una sociedad tradicionalmente violenta. Así, a diferencia de muchos otros países, en Colombia es muy probable que lo que sucede en internet tenga graves consecuencias en el mundo real. De hecho, en varias ocasiones las redes sociales han sido el espacio inicial para intimidar y amenazar a víctimas de futuros ataques físicos.[26] Por lo tanto, en Colombia es urgente poner en práctica una alfabetización digital enfocada en fomentar una cultura de protección a la intimidad.

6. Política pública de seguridad digital — CONPES

Actualmente Colombia afronta un proceso de formulación de política pública de seguridad digital que incluye por lo pronto un compromiso del Gobierno con el respeto a los derechos humanos. Sin embargo, el documento y las múltiples acciones concretas que prevé no desarrollan este compromiso, en especial en lo relacionado con la preservación de la intimidad. Los lineamientos de política pública carecen de un enfoque que incluya el contexto específico de justicia transicional que vive la sociedad colombiana. El enfoque del documento, en cambio, está puesto en la seguridad bancaria y comercial, mas no en las injerencias arbitrarias o ilegales en la intimidad de las personas, especialmente defensores de derechos humanos, víctimas del conflicto armado, periodistas, opositores políticos, etc. Estos lineamientos carecen además de un diagnóstico de los abusos y graves violaciones a la privacidad de la ciudadanía llevadas a cabo por los organismos de inteligencia del Estado como una amenaza a la seguridad digital. Sumado a ello, no prevé facultades específicas de control a los jueces en materia de protección a la intimidad en el entorno digital. Estos lineamientos tampoco incorporan los estándares nacionales e internacionales de protección a los datos personales frente a las nuevas tecnologías de comunicaciones y vigilancia.

Señor Relator, por los puntos anteriormente referenciados consideramos que el ejercicio de su mandato será estratégico para impactar positivamente la promoción del derecho a la intimidad en Colombia, por lo que nos ponemos a su entera disposición para ampliar o precisar el contenido del presente documento.

Cordialmente,

Fundación Karisma Dejusticia

[1] Ley de actividades de inteligencia y contrainteligencia. Ley 1621 de 2013, artículo 17. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1621_2013_pr001.html#44.
[2] Decreto 1704 de 2012. Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=48863
[3] Ley 1621 de 2013.
[4] Castañeda, J. (2016). *Is data retention legitimate in Colombia?*. Available on https://karisma.org.co/descargar/is-data-retention-legitimate-in-colombia/.
[5] Ley 1621 de 2013, artículo 19.
[6] Privacy International. (2015). *Shadow State: Surveillance, Law and Order in Colombia*. Available on https://www.privacyinternational.org/node/635.
[7] Ley 418 de 1997. Available on http://www.secretariasenado.gov.co/senado/basedoc/ley_0418_1997_pr002.html#102. This act was extended by Ley 1738 de 2014. Available on http://www.secretariasenado.gov.co/senado/basedoc/ley_1738_2014.html#1. On the subject, *see* Castañeda, J. (2015, January 2015). The dangerous ambiguity of communications encryption rules in Colombia. *Digital Rights Latin American and the Caribbean*, 19. Available on http://www.digitalrightslac.net/en/la-peligrosa-ambiguedad-de-las-normas-sobre-cifrado-de-comunicaciones-en-colombia/
[8] Ley 1621 de 2013, artículo. 44, párrafo 2.
[9] Botero, C. & Sáenz, P. (2015, August 24). In Colombia, PUMA is not what it seems. *Digital Rights Latin American and the Caribbean*, 26. Available on http://www.digitalrightslac.net/es/en-colombia-el-puma-no-es-como-lo-pintan/.
[10] Newman, V. (2015, July 10). *El hackeador hacheado*. Available on http://www.dejusticia.org/#!/actividad/2667; Castañeda, J. (2016, 12 January). *When the state hacks*. Available on https://karisma.org.co/when-the-states-hacks/.
[11] Roban expedientes de restitución de tierras. (2015, July 9). *El Pilón*. Available on http://elpilon.com.co/roban-expedientes-de-restitucion-de-tierras/.
[12] Ley 1581 de 2012. Available on http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.
[13] Ley 1621 de 2013, artículo 33; Decreto 857 de 2014, artículos 5, 6 y 10.
[14] Privacy International. (2015). *Shadow State: Surveillance, Law and Order in Colombia.* Available on https://www.privacyinternational.org/sites/default/files/ShadowState_English.pdf.
[15] Restrepo, J.D. (2007, August 30). Medellín, un laboratorio óptimo de las 'chuzadas' telefónicas. *Revista Semana*. Available on http://www.semana.com/on-line/articulo/medellin-laboratorio-optimo-chuzadas-telefonicas/87938-3.
[16] Plataforma Puma de la Policía entrará en operación, pero limitada. (2015, September 30). *El Tiempo*. Available on http://www.eltiempo.com/politica/justicia/plataforma-unica-de-monitoreo-y-analisis-comienzan-pruebas/16390794.
[17] El DAS sigue grabando. (2009, February 21). *Revista Semana*. Availbale on http://www.semana.com/nacion/articulo/el-das-sigue-grabando/100370-3.
[18] Fondo de Vigilancia y Seguridad. (2015). *Informe de gestión enero — diciembre de 2015*. Available on http://www.fvs.gov.co/portal/attachments/article/104/INFORME%20GESTIÓN%20ENERO-DICIEMBRE%202015.pdf.
[19] Ley 1241 de 2009, artículo 22(21). Available on http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html#22.
[20] Resolución 0912 de 2008 de la Policía Nacional. Available on https://www.redjurista.com/documents/r_mdef_0912_2008.aspx.

[21] Programa Somos Defensores. (2015). *Los Nadie. Informe enero — junio 2015*. Colombia: pp. 50-51. Available on http://somosdefensores.org/attachments/article/134/los-nadie-informe-semestral-siaddhh2015.pdf; Programa Somos Defensores. (2014). *Informe Especial: protección 'Al Tablero'*. Colombia: p. 17. Available on http://somosdefensores.org/attachments/article/88/proteccion_al_tablero_version_eb.pdf.

[22] Programa Somos Defensores (2015) *La divina comedia. Informe Anual 2014*. Colombia: pp. 63-67. Available on http://www.somosdefensores.org/attachments/article/132/la-divina-comedia-web-final.pdf.

[23] Fundación para la Libertad de Prensa. (2014). *60 años de espionaje a periodistas en Colombia. Informe sobre el estado de la libertad de prensa en 2014*. Available on http://flip.org.co/sites/default/files/archivos_publicacion/Informe%20Anual%202014%20FLIP_0.pdf.

[24] Fundación para la Libertad de Prensa. (2015). *Paz en los titulares. Miedo en la redacción. Informe sobre el estado de la Libertad de Prensa en Colombia en 2015*. Available on http://flip.org.co/sites/default/files/archivos_publicacion/Informe%20Anual%202015%20V.%20Final.pdf.

[25] Fundación para la Libertad de Prensa. (2015). *Tercera encuesta nacional a periodistas sobre libertad de expresión y acceso a la información*. Available on http://flip.org.co/es/content/tercera-encuesta-nacional-periodistas-sobre-libertad-de-expresi%C3%B3n-y-acceso-la-informaci%C3%B3n.

[26] Toledo, A. (2016). *Misoginia en internet: bombardeo a campo abierto contra las periodistas*. Available on https://karisma.org.co/misoginia-en-internet-bombardeo-a-campo-abierto-contra-las-periodistas/.