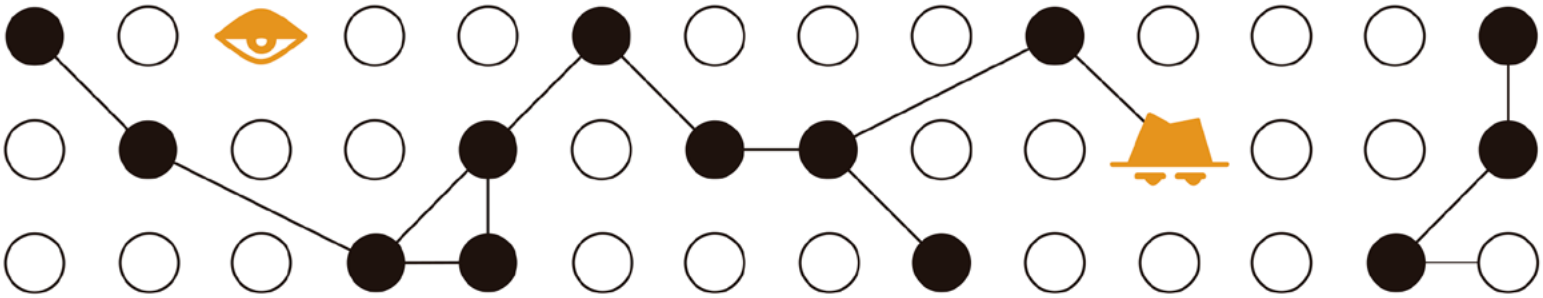

¿ES LEGÍTIMA LA RETENCIÓN DE DATOS EN COLOMBIA?

ANÁLISIS COMPARATIVO DE UNA HERRAMIENTA DE VIGILANCIA MASIVA QUE RESTRINGE LOS DERECHOS HUMANOS

Fundación Karisma

Por Juan Diego Castañeda

Elaborado por:
Fundación Karisma
karisma.org.co

Con el apoyo de Privacy International

PRIVACY INTERNATIONAL

Fundación Karisma
www.karisma.org.co

Enero de 2016

"En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesible, es decir, tienen un formato electrónico diseñado para que su contenido pueda ser leído por el mayor número de personas posible, incluidas las que tienen algún tipo de discapacidad o de dificultada para la lectura y comprensión. Más información sobre el tema: http://www.documentoaccesible.com/#que-es

Consulta este análisis en línea en:

https://karisma.org.co/es-legitima-la-r…atos-en-colombia/

Tablas de Contenido

Introducción

Las preocupaciones por seguridad nacional y por la creciente actividad criminal en línea se han convertido en justificación para la vigilancia de las autoridades a las tecnologías de la información y las comunicaciones (TIC), sin embargo, no cualquier actividad de inteligencia por los Estados es legal, ni legítima. Es necesario analizar las nuevas técnicas de vigilancia y revisar los marcos jurídicos de los países para asegurarnos de que estén en línea con los derechos humanos.

La vigilancia estatal de las comunicaciones busca recaudar datos para la investigación de inteligencia o criminal. En ese proceso, las actividades se ocupan de la recolección, almacenamiento, procesamiento y circulación de datos y comprende diferentes técnicas. Las técnicas más comunes son la interceptación de comunicaciones, la retención de datos y el uso de herramientas de hackeo (p. Ej. pruebas de penetración y explotación de vulnerabilidades de seguridad). Sin embargo, la falta de un proceso democrático en la creación de capacidades de vigilancia y el establecimiento de fuertes controles y medidas de transparencia pueden ser ilegales y ocasionar graves violaciones a derechos humanos, comprometiendo así las bases mismas de la democracia[1].

En este documento se analizan las normas colombianas sobre retención de datos y se las compara con Perú, México y Brasil desde el punto de vista del cumplimiento de los estándares internacionales para el establecimiento de medidas de restricción de derechos fundamentales, especialmente de la libertad de expresión y la intimidad. Dada la particularidad del caso Argentino, no se hace la comparación general pero sí donde corresponda.

El propósito central es el de revisar el alcance de la protección de los derechos humanos en el marco de las normas de retención de datos colombianas y respecto de sus equivalentes en la región y de los estándares relevantes dentro del Sistema Inte-

ramericano de Derechos Humanos fue principalmente el Informe del año 2013 de la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA. La pregunta central es ¿Es el marco legal colombiano de retención de datos un marco garantista dentro del contexto regional?

La investigación de los marcos legislativos en cada país tuvo como insumo de base los informes coordinados por Katitza Rodríguez de la Electronic Frontier Foundation para Perú[2], México[3], Brasil[4], Colombia[5] y Argentina[6].

¿Qué requiere una restricción de derechos fundamentales para ser legítima?

Según la Relatoría para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, las medidas que afectan las comunicaciones, en tanto restricciones a derechos fundamentales, deben ser acordes con estándares y principios planteados en distintos documentos internacionales y los Estados deben revisar y armonizar sus normas según ellos.

Según el Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la Libertad de Opinión y Expresión, se entiende que a pesar de que el artículo 17 del Pacto Internacional de los Derechos Civiles y Políticos no especifica las condiciones que debe seguir las limitaciones al derecho a la intimidad, es claro que toda limitación a este derecho debe cumplir con las garantías establecidas para otros derechos. Así pues, las limitaciones admisibles a la intimidad (a) deben ser legales, (b) no deben comprometer la esencia del derecho humano, (c) deben ser necesarias en democracia, (d) no deben ser discrecionales, (e) deben ser necesarias para un objetivo legítimo, y (f) deben ser proporcionales, adecuadas, las menos lesivas y deben guardar proporción con el interés protegido.

El Relator para libertad de expresión de la OEA, a propósito de las revelaciones sobre el uso de productos y servicios de la empresa italiana Hacking Team por parte de gobiernos alrededor del mundo[7], expresó que:

> de acuerdo con los estándares internacionales, el uso de programas o sistemas de vigilancia en las comunicaciones privadas debe estar establecido de manera clara y precisa en la ley, ser verdaderamente excepcional y selectivo, y estar limitado en función a lo estrictamente necesario para el cumplimiento de fines imperativos como la investigación de delitos graves definidos en la legislación[8].

Finalmente, hay que tener en cuenta los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones,* que fueron desarrollados a partir de las conceptualizaciones que se han realizado en torno al derecho internacional de los derechos humanos en el entorno digital[9] en un proceso que distintas organizaciones de la sociedad civil lideraron y que contó con la participación de representantes de la industria y expertos en la materia. Los principios que deben regir la aplicación de medidas de vigilancia de las comunicaciones son: legalidad, objetivo legítimo, necesidad, idoneidad, proporcionalidad, autorización judicial competente, debido proceso, notificación del usuario, transparencia, supervisión pública, integridad de las comunicaciones y los sistemas, garantías para la cooperación internacional y garantías contra el acceso ilegítimo, y derecho a un recurso efectivo.

En esencia, los requisitos por los que nos guiaremos en este documento serán los resumidos por la Relatoría para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, que indican que una medida de vigilancia de las comunicaciones es legítima si la medida[10]:

1. Está establecida en una ley
2. Persigue un objetivo imperativo
3. Es necesaria, idónea y proporcional respecto al objetivo que persigue
4. Se respeta el debido proceso y reserva judicial

En lo que sigue se explicará por qué la retención de datos es una medida que restringe derechos fundamentales y veremos cada uno de estos requisitos y cómo está la ley Colombiana frente a ellos.

¿Qué es la retención de datos y por qué es una restricción a derechos fundamentales?

Nuestros datos más personales, los que mejor pueden reflejar nuestra vida e incluso nuestros pensamientos ya no permanecen exclusivamente en nuestra esfera íntima. Ahora la información personal también se encuentra en bases de datos, que tiene diversos fines y son administradas por entidades públicas o privadas. Esas bases de datos están siendo alimentadas por flujos de información constantes. Su conjunto conforma un archivo sobre cada individuo, un "dossier personal[11]". Las tecnologías digitales de las que la vida moderna depende, como computadores personales, teléfonos celulares y demás, producen y registran datos constantemente. Los computadores registran a qué horas están encendidos, qué aplicaciones se usan, las páginas web que se visitan, el lugar donde se encuentran. Los celulares están todo el tiempo atentos a su ubicación geográfica, contienen registros de llamadas entrantes y salientes, mensajes de texto y fotos. La fuerza de estos datos radica en su combinación: un análisis de datos a partir del cruce de distintas bases de datos puede llegar a revelar tanto sobre una persona que puede convertirse en una seria violación de sus derechos. Sin embargo, todo esto hace parte de una suerte de concesión que hacen las personas usuarias a cambio de recibir el servicio. El resultado, en términos del tipo de datos que producimos y quienes los administran, es que somos un "libro abierto para los gobiernos y las corporaciones[12]". De ahí que se necesite garantizar el respeto a los derechos humanos que pueden afectarse por estos flujos y usos de la información.

La provisión de servicios de telecomunicaciones es uno de los ámbitos donde se producen más datos y, gradualmente, más gobiernos obligan a estos proveedores a retenerlos y entregarlos para diversos propósitos. El interés de los gobiernos en este punto radica, principalmente, en que las personas usuarias tienen una relación de dependencia con las empresas de telecomunicaciones en dos niveles: (1) el de la provisión

del servicio en sí misma, y (2) el de la salvaguarda de los datos que fluyen a través de la conexión[13]. Las obligaciones de retención buscan la conservación de los datos que generan las conexiones de telefonía fija, celulares o de Internet, estableciendo el tipo de datos a conservar por los operadores, el tiempo de retención y las condiciones, y los facultados para el acceso a esos datos.

Los datos que se recogen son, por ejemplo, el número que recibe una llamada, el tiempo de la llamada, la ubicación geográfica del dispositivo o sus identificadores únicos (IMEI e IMSI) en telefonía móvil o fija, y las direcciones IP en internet. Esto es, en un nivel simple, diferente de la recolección de las comunicaciones en sí mismas y, por tanto, han sido llamados "metadatos", es decir, datos acerca de los datos de comunicación. Esta clasificación puede llevar a concluir erróneamente que los metadatos o los datos de identificación del suscriptor merecen una protección menor a la que está establecida para las comunicaciones en sí mismas[14]. La agregación de datos, en realidad, es más reveladora que el contenido de las comunicaciones[15]. Por esta razón, se ha establecido que la retención de datos es una medida que restringe y afecta los derechos a la intimidad y a la libertad de expresión[16].

A continuación vamos a explicar los requisitos de (1) legalidad, (2) objetivo imperativo, (3) necesidad, idoneidad y proporcionalidad y (4) control judicial y debido proceso. En cada uno de ellos haremos el análisis de la regulación colombiana y la compararemos con las retención de datos que existe en Perú, México y Brasil.

I.Legalidad

Una restricción a los derechos a la intimidad o a libertad de expresión como la que comporta la retención obligatoria de datos de telecomunicaciones debe (1) estar consignada en una ley en sentido formal y material, y (2) debe ser clara y precisa[17].

Ley en sentido formal y material

Sobre el primer punto, está claro que solo se cumple el requisito cuando la restricción se impone a través de una norma adoptada por el órgano legislativo democráticamente elegido y según el procedimiento previsto en la constitución respectiva. Una disposición administrativa no satisfaría el requisito.

En los ordenamientos analizados, se encuentra una mezcla de regulaciones y leyes en sentido material que aplican distintos aspectos de la retención de datos.

En Colombia, la retención de datos está establecida en dos normas:

1. El Decreto No. 1704 de 2012, que trata de la retención de datos para efectos de investigación criminal.

2. La Ley No. 1621 de 2013, que lo hace para efectos de actividades de inteligencia.

En ese sentido, Colombia no está tan lejos de los demás países analizados pues desafortunadamente combina leyes en sentido formal y material con decretos y regulaciones.

Perú: La Ley No. 27.336 (2002) regula la conservación de registros fuentes del detalle de las llamas y facturación de los servicios. El Decreto Legislativo No. 1182 (2015) regula la retención de datos de tráfico y de identificación y localización de terminales y El Código Procesal Penal (Decreto Legislativo No. 957 de 2004) regula el acceso a la geolocalización de dispositivos por parte del organismo investigador.

Brasil: En Brasil se encuentran dos resoluciones administrativas que regulan la retención de datos de telefonía fija (Resolución No. 426/05 de ANATEL) y móvil (Resolución No. 477/07 de la misma entidad), la Ley No. 12.850 sobre retención y acceso a datos en ambas modalidades de telefonía, y la Ley No. 12.965 o Marco Civil de Internet, sobre retención y acceso a datos de tráfico de Internet.

México: Este país es una excepción en este punto pues el régimen de retención está enteramente consagrado en leyes en sentido formal y material a través de la Ley Federal de Telecomunicaciones y Radiodifusión (2014) y del Código Nacional de Procedimientos Penales (CNPP), que sustituye al Código Federal de Procedimientos Penales (CFPP).

Argentina: Hay dos cosas que merecen ser mencionadas en este punto. La primera, en este país no hay consagración legal expresa de la retención de datos. Sin embargo, se encuentra vigente el Reglamento de calidad de los servicios de telecomunicaciones de la Secretaría de Comunicaciones -ahora Autoridad Federal de las Tecnologías de la Información y las Comunicaciones-, que obliga a los prestadores a garantizar a la autoridad toda la información que estime pertinente para hacer las evaluaciones de calidad del servicio[18]. Así mismo, su artículo 8 obliga directamente a la conservación de los datos que recojan sus sistemas y que puedan servir para determinar la calidad del servicio.

La segunda es que es el único caso en el que la retención de datos para efectos de investigación criminal fue declarada inconstitucional. La Ley No. 25.873 y su decreto reglamentario No. 1563 de 2004 obligaban a los prestadores de servicios de telecomunicaciones a "registrar y sistematizar los datos filiatorios y domiciliarios de sus usuarios y clientes y los registros de tráfico de comunicaciones cursadas por los mismos" por el plazo de 10 años y para acceso del Poder Judicial o del Ministerio Público. Estas normas fueron declaradas inconstitucionales por la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal por violar los requisitos de legalidad y necesidad y proporcionalidad.

El Tribunal consideró que resulta inadmisible la vaguedad de la invocación del interés general para sustentar las normas en cuestión, en vista de la afectación que comportan a los intereses de la ciudadanía[19]. Respecto al requisito de legalidad, opinó que no está claro qué son datos de tráfico, por tanto, podría confundirse con el contenido de la comunicación. Además, determinó que no había claridad sobre las condiciones y las autoridades que tendrían acceso a los datos. Dejó claro que, en todo caso, el acceso a los datos requeriría autorización judicial.

También se pronunció respecto a la proporcionalidad de la medida y dijo que "no es dudoso que la norma en cuestión pone bajo sospecha a todos los usuarios de los servicios de telecomunicaciones por el amplísimo término de 10 años", lo que se agrava en el ámbito de las comunicaciones digitales porque allí "todos los movimientos quedan registrados". Señaló, además, que la medida no era admisible porque, aunque no todos los procedimientos podrían ameritar su uso, no está claro para qué procedimientos judiciales estaba autorizada.

Claridad

Como parte del requisito de legalidad, los regímenes de retención de datos deberían ser claros respecto al tipo de datos afectados por la medida y al tiempo por el que deben ser retenidos. En Colombia, para el caso de investigación criminal, se obliga a los proveedores de servicios de telecomunicaciones a conservar la información del suscriptor y los datos que permitan saber la localización de terminales en tiempo real[20]. En el caso de las actividades de inteligencia, se pide la retención del "historial de comunicaciones de los abonados telefónicos vinculados, los datos técnicos de identificación de los suscriptores sobre los que recae la operación" y los datos de localización[21].

No está claro qué significa "historial de comunicaciones" ni el alcance de las cláusulas generales empleadas en estas normas (p. ej "entre otras" o "cualquier otra información"). Sobre el tiempo, en ambos casos los datos deben ser retenidos por el término de 5 años, aunque no está claro si los datos de localización deben ser registrados para posterior consulta.

En el resto de países también hay serias faltas de claridad. Por ejemplo, en Perú no está claro qué se entiende por "datos derivados de las telecomunicaciones"[22], ni tampoco qué son exactamente los datos de localización[23]. En Brasil se exige vagamente la retención de "todos los datos relativos a la prestación del servicio, incluidos los de facturación[24]". México en cambio hace una lista exhaustiva de los datos que son materia de retención, que van desde los del suscriptor hasta el registro de la hora de inicio y finalización de la comunicación y los números involucrados[25].

Por otro lado, en Colombia tampoco está claro si la obligación de retención aplica también a los datos de tráfico de Internet, pues, aunque los artículos relevantes, tanto

del Decreto 1704 como de la Ley 1621, se dirigen a los "proveedores de redes y servicios de telecomunicaciones" u "operadores de servicios de telecomunicaciones", los datos que se menciona parecen estar relacionados solo con la telefonía móvil o fija.

Brasil es quizás la legislación más clara en este punto pues tiene regulaciones o legislación específica para cada canal de comunicación, es decir, para telefonía fija, móvil e Internet.

Hechos y autoridades

Dentro del requisito de legalidad se exige que una medida de restricción de derechos fundamentales como la retención de datos sea clara respecto a las circunstancias que ameritan la recolección o el acceso a los datos, sobre las autoridades facultadas para acceder, las condiciones que deben comprobarse para realizar el acceso y las autoridades a quienes corresponde el control de la medida.

En Colombia, respecto a la investigación penal, cualquier investigación amerita el acceso a los datos retenidos. La orden de entrega debe provenir de la Fiscalía General de la Nación y la ejecución de la orden está en manos del "grupo de Policía Judicial" designado[26]. En cuanto a las actividades de inteligencia, la única restricción que impone la norma es la existencia de una "operación autorizada", aunque no hay forma de determinar qué hechos ameritan el desarrollo de una operación de inteligencia ni quién puede autorizarla. Además, con una norma tan ambigua, hay un buen número de autoridades que podrían legítimamente solicitar esta información por ser parte de la comunidad de inteligencia[27].

México es otro mal ejemplo en cuanto a las autoridades que pueden acceder a los datos. La Ley Federal de Telecomunicaciones y Radiodifusión (art. 189) trae una cláusula general según la cual los "proveedores de servicios de aplicaciones y contenidos están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes". Tanto los datos de tráfico como los de localización deben ser entregados según la LFTR, de forma vaga, a "las autoridades competentes", lo que incluye las "instancias de seguridad y procuración de justicia", por remisión al artículo 189 (fracción III del artículo 190, inciso primero).

Específicamente, el Código Federal de Procedimientos Penales (Art. 133 Quáter) determina que la Procuraduría General de la República puede solicitar el acceso a datos de geolocalización en tiempo real cuando se investiguen hechos de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas. Sin embargo, el Código Nacional de Procedimientos Penales (Art. 291), que reemplazará al CFNP, deja abierta la posibilidad a que cualquier investigación haga uso del acceso a datos de localización.

Brasil tiene los mismos problemas, incluso respecto a los datos de internet: el Marco Civil de Internet no especifica cuales son las autoridades que pueden acceder a la información retenida. Por una parte, dice (artículo 10, párrafo 3) que las "autoridades administrativas que tengan competencia legal" podrán acceder a la información del suscriptor. Por otra, el artículo 22 establece que el acceso a registros de conexión y acceso a aplicaciones de Internet serán autorizados a "la parte interesada" en la recolección de material probatorio en investigaciones civiles o penales.

Respecto a las razones y condiciones para acceder a los datos, Perú es más específico que los demás países cuando se trata de los datos de geolocalización de celulares. La normativa determina que una unidad especializada de la Policía para la petición de datos podrá acceder cuando concurran las siguientes condiciones[28]: (1) cuando se trate de flagrancia, (2) cuando el delito investigado sea sancionado con pena superior a los cuatro años de privación de libertad, y (3) cuando el acceso a los datos constituya un medio necesario para la investigación. La Fiscalía, por su parte, podrá acceder a los datos de geolocalización cuando investigue la posible comisión de una conducta sancionada con una pena privativa de la libertad mayor a 4 años y bajo la convicción de su absoluta necesidad[29].

II. Objetivos imperativos

El segundo requisito que debe cumplir una medida de restricción de derechos fundamentales es que se establezca para alcanzar ciertos objetivos imperativos autorizados por la Convención Americana. Estos objetivos son (1) protección de los derechos de los demás, (2) seguridad nacional, (3) orden público, (4) salud pública, y (5) moral pública. La interpretación de estos objetivos debe estar de acuerdo con los principios de una sociedad democrática. Es decir, los Estados no pueden interpretarlos libremente[30].

La protección de los derechos de los demás requiere que la amenaza sea clara y que la medida no se imponga para proteger los mismos derechos que afecta. Asimismo, debe recurrirse a medidas menos restrictivas antes de afectar derechos[31].

El mantenimiento del orden público, en tanto "condiciones que aseguran el funcionamiento armónico y normal de las instituciones sobre la base de un sistema coherente de valores y principios", requiere que se demuestren "causas reales y objetivamente verificables, que planteen una amenaza cierta y creíble de una perturbación potencialmente grave de las condiciones básicas para el funcionamiento de las instituciones democráticas". No valen, entonces, las justificaciones sobre hechos o situaciones hipotéticas o amenazas sin el adecuado nivel de gravedad[32].

La seguridad nacional, por su parte, no debe definirse en términos incompatibles con una sociedad democrática. Por ejemplo, justificando ataques a disidentes políticos, periodistas o defensores de derechos humanos con objetivos políticos o para entorpecer su trabajo. Los criterios para considerar que un caso amerita aplicación de la medida deben estar claramente definidos[33].

Como se puede deducir del análisis del requisito de legalidad, las legislaciones estudiadas, incluida la colombiana, no obedecen completamente el requisito de la persecución de objetivos imperativos para la imposición de la medida de retención de datos. Por ejemplo, las regulaciones de Brasil (resoluciones no. 426/05 y 477/07) y Perú (Ley No. 27.336) ordenan la medida para efectos de control de las empresas de prestación de servicios de telecomunicaciones, a la vez que garantizan el acceso a esos datos a organismos de seguridad. La legislación mexicana simplemente ordena la retención de datos en el marco de una ley que regula de manera general el sector de las telecomunicaciones, sin hacer una referencia expresa a los motivos de la retención.

La legislación colombiana, aunque impone la retención y garantiza el acceso a datos solo en el marco de una investigación criminal o las actividades de inteligencia, está muy lejos de determinar con claridad la amenaza a la seguridad nacional o al orden público que la medida puede llegar a minimizar. Las agencias de inteligencia pueden tener acceso a los datos retenidos a través de cláusulas generales, lo que efectivamente implica la imposición de medidas de restricción con objetivos que no son imperativos ni urgentes y la violación del principio de legalidad. Por tanto, no hay ninguna certeza sobre el alcance y los hechos que justifican la medida. México se destaca por tener en la Ley de Seguridad Nacional una lista de qué se considera como amenazas a la seguridad nacional (Art.5).

El siguiente requisito trata de la necesidad, idoneidad y proporcionalidad de una medida *para alcanzar los objetivos imperativos*. Por eso si la conexión entre la medida y los objetivos no es suficiente, como es el caso de las legislaciones analizadas, será muy difícil decir que la medida es necesaria, idónea y proporcional.

III. Necesidad, Idoneidad y Proporcionalidad

El tercer requisito que debe cumplir una medida de restricción de derechos fundamentales para ser considerada legítima es que se demuestre su necesidad, idoneidad y proporcionalidad.

La necesidad de una medida de restricción de derechos debe ser cierta y urgente, lo que, además, impone una demostración más allá de lo simplemente útil, razonable u oportuno para alcanzar los objetivos imperativos. Además, la medida debe estar limitada a lo indispensable para alcanzar el objetivo por lo cual debe considerarse la

imposición de medidas menos restrictivas. Por tanto, la medida debe estar autorizada solo para casos excepcionales[34].

La retención de datos, por naturaleza, y tal como aparece en las legislaciones analizadas, es una medida que afecta los derechos a la intimidad y a la libertad de expresión, entre otros, y opera de manera constante sobre los datos de las personas usuarias de servicios de comunicaciones. Esa pasividad de la medida excluye por completo el requisito de necesidad, pues no opera solo en casos excepcionales. Por otro lado, la vaguedad con la que está consagrado en las normas, el acceso a los datos retenidos tampoco permite pensar que la medida se usa excepcionalmente. En Colombia, se puede acceder a todos los datos que se debe retener para la investigación de cualquier delito o para cualquier situación que los organismos de inteligencia consideren necesaria. Lo mismo sucederá en México cuando entre a regir el Código Nacional Procesal Penal. En Perú y Brasil, las cláusulas generales de colaboración con los organismos de inteligencia impiden determinar cuáles son los casos excepcionales en los que se usará la medida.

El requisito de idoneidad busca que la medida sea "efectivamente conducente para obtener los objetivos legítimos e imperiosos que mediante ella se persiguen[35]". Como queda claro del análisis, la falta de precisión en los términos de la medida y la ausencia de conexión fuerte entre ella y los objetivos imperativos impide determinar su idoneidad.

La proporcionalidad nace de evaluar (1) el grado de afectación a derechos que supone la medida, (2) la importancia de satisfacer el derecho protegido por la medida, y (3) si tal satisfacción de ese derecho justifica la restricción de los otros[36]. La aplicación de medidas de vigilancia de las comunicaciones deberá autorizarse solo ante la presencia de riesgo cierto contra los derechos protegidos (seguridad, por ejemplo), y cuando el interés de la sociedad en mantener esos derechos sea superior al de mantener los derechos que afecta[37].

Establecer la proporcionalidad de la medida en cada legislación de forma abstracta es difícil, ya que requiere de la evaluación de sus contextos sociales, culturales y legales particulares. Sin embargo, debe tenerse en cuenta que estas legislaciones implican la retención de todos o de algunos de estos datos: información de la persona suscrita al servicio, datos de tráfico de comunicaciones fijas, móviles y de Internet, y la localización de las terminales; que el número de autoridades que pueden acceder a ellos es amplio y que los motivos que justifican el acceso tampoco son claros. Además, el tiempo de retención parece ser arbitrario. En Colombia, la única mención establece 5 años, lo que obligaría a pensar que se refiere a cualquier tipo de datos. En Perú, se establecen 3 años, mientras que en México son 2 años. En Brasil, los datos de telefonía móvil o fija deben retenerse por 5 años y los de Internet por 1 año.

Por el momento, solo en Brasil se está discutiendo ante las Cortes la legalidad y proporcionalidad de la medida de retención impuesta en la Ley No. 12.850 sobre crimen organizado, pues, a juicio de las personas accionantes, no hay claridad respecto a la necesidad de autorización judicial para el acceso a datos de tráfico, situación que aprovechan las autoridades para exigir toda clase de datos retenidos por los operadores.

Los argumentos con los que el Tribunal de Justicia de la Unión Europea declaró la invalidez de la Directiva 2006/24/EC sobre retención de datos son relevantes, pues apuntan a muchos de los problemas que tienen los regímenes de retención de datos analizados en este documento[38]. Sobre la proporcionalidad de la medida, señala el fallo que su población objetivo resulta ser cualquier persona que haga uso de medios de comunicación, es decir, toda la población europea. En ese contexto, el Tribunal no encuentra que haya límites a la aplicación de la medida en función del objetivo que persigue. En particular, no hay límites a las zonas geográficas, personas o tipos de comunicaciones sujetas a la medida en relación con el objetivo que persigue o la gravedad de los hechos que se investigan.

Descontando la legitimidad de la retención de datos para efectos de control de los prestadores del servicio de telecomunicaciones (Perú y Brasil) o para efectos indeterminados (México), no se encuentran límites adecuados a la medida cuando se emplea para investigación criminal y para suministrar información a los organismos de inteligencia. No existe ningún tipo de límite respecto a las personas ni al tiempo que pueden ser afectadas. En Colombia ni siquiera hay una limitación respecto al tipo de delitos cuya investigación puede servirse de datos retenidos.

En estas condiciones, la proporcionalidad de la retención de datos queda claramente cuestionada, pues los intereses de la sociedad en la investigación de los delitos, por sí mismos, no justifican una afectación de semejante magnitud en los derechos a la intimidad y a la libertad de expresión de las personas donde esta se encuentra vigente. A esto debe sumarse que la efectividad de la retención de datos radica, si acaso, en la facilitación de la investigación de hechos pasados, aunque poco pueda hacer para prevenir la comisión de crímenes en el futuro[39].

IV. Debido proceso y reserva judicial

Una medida de restricción de derechos, para ser legítima, debe respetar "las garantías vinculadas al debido proceso y a la reserva judicial[40]". Esto comprende, en general, la posibilidad de autorización y control judicial, la notificación a la persona usuaria afectada por la medida y la presentación de informes de transparencia sobre el empleo de la medida.

Reserva judicial

Las normas sobre retención de datos deberían ser claras respecto a las condiciones que admiten el acceso a los datos retenidos y las autoridades que pueden hacerlo. Cuando existen estos requisitos, son las autoridades judiciales las llamadas a decidir si la medida es: idónea para alcanzar el objetivo, suficientemente restringida para no vulnerar derechos más de lo necesario, y proporcional respecto al interés defendido[41]. En pocas palabras, son las autoridades judiciales quienes deben velar por la aplicación de las medidas que restringen derechos en el marco constitucional y democrático.

A diferencia de la interceptación de comunicaciones, la retención de datos es automática y abarca a toda la población. Por tanto, la actividad misma de recolección de datos no requiere la valoración judicial previa de su necesidad y proporcionalidad. Respecto al control judicial del acceso a los datos retenidos o a los datos de geolocalización, la regla varía de país a país.

A diferencia de lo que sucede en otros países, en Colombia el acceso a los datos retenidos o a la geolocalización de dispositivos no requiere ningún tipo de autorización judicial. Tampoco está sometida a control judicial posterior ni en el contexto de la investigación criminal ni en el de las actividades de inteligencia. En México, similar a lo que sucede en Colombia, el acceso a datos de tráfico retenidos en virtud de la LFTR y a los de geolocalización (Código Federal de Procedimientos Penales) no requiere autorización judicial. El Código Nacional de Procedimientos Penales sí requerirá autorización judicial para acceder a la geolocalización.

En cambio, Perú requiere que la Policía solicite autorización judicial para acceder a los datos de tráfico retenidos (Segunda disposición complementaria final del Decreto No. 1182), a los datos de geolocalización (Decreto No. 1182. Artículo 5). Lo mismo deben hacer los organismos de Inteligencia (artículo 32 del Decreto No. 1141).

Brasil, aunque no es claro respecto a lo que debe hacerse para los datos de telefonía, establece que el acceso a los registros de conexión y aplicaciones de Internet será autorizado por un juez solo para investigaciones penales o civiles cuando haya (1) indicio fuerte de culpabilidad, (2) justificación de la utilidad de los registros en la investigación, y (3) se especifique el período por el cual se solicitan los registros[42].

Notificación a la persona usuaria

Este requisito también incluye las garantías procesales para que las personas afectadas por la medida puedan defenderse adecuadamente[43]. Por tanto, notificar a la persona usuaria es parte esencial de su defensa, ya que o de otra manera no podría saber si ha sido vigilado y presentar los recursos adecuados para mitigar los efectos de la vigilancia.

El único país que prevé la notificación a la persona usuaria en un caso es Perú, en específico, para los casos de acceso a datos de localización a través del procedimiento del artículo 230 del Código Procesal Penal. Tal notificación está contemplada para realizarse posteriormente a la puesta en marcha de la medida y solo "si el objeto de la investigación lo permitiere y en tanto no pusiere en peligro la vida o la integridad corporal de terceras personas", asunto que determinará el juez correspondiente (Art. 231). Sin embargo, este procedimiento no está establecido en el Decreto No. 1182 ni en la Ley No.27.336.

Transparencia

Para efectos de que las actividades de vigilancia de los Estados sean transparentes y que la ciudadanía pueda ejercer el debido control, se requiere que los Estados publiquen "información global sobre el número de solicitudes de intercepción y vigilancia aprobadas y rechazadas, incluyendo la mayor cantidad de información posible como – por ejemplo – un desglose de solicitudes por proveedor de servicios, tipo de investigación, tiempo durante el cual se extienden las investigaciones, etcétera[44]". Asimismo, los proveedores de servicios de telecomunicaciones deberían publicar informes donde especifiquen qué procedimientos siguen cuando reciben una solicitud de las autoridades, el tipo de solicitudes y su cantidad[45].

México es el único país que dispone sobre la publicación de informes de transparencia. EL Artículo Art 70 XLVIII de la La Ley General de Transparencia y Acceso a la Información Pública obliga a las autoridades a publicar el listado de solicitudes que han hecho a concesionarios y proveedores de servicios y aplicaciones de Internet respecto a intervención de comunicaciones y registros de datos y geolocalización. El informe debe contener, a saber,: el objeto de la intervención, el alcance temporal, sus fundamentos legales y la existencia de autorización judicial, cuando sea el caso.

Los prestadores de servicios de telecomunicaciones podrían estar obligados a presentar un informe semestral sobre las solicitudes de acceso a datos de tráfico y de geolocalización, especificando el número de solicitudes recibidas, aceptadas y rechazadas. Esto sería así si queda en firme el lineamiento décimo cuarto del Borrador de "Lineamientos de colaboración en materia de seguridad y justicia", que presentó el Instituto Federal de Telecomunicaciones a partir de la facultad que le otorga el artículo 190 I de la LFTR.

Conclusiones

A juzgar por los estándares internacionales para la protección de derechos humanos en la vigilancia de las comunicaciones que hemos visto acá, la retención de datos es ilegítima. Esto es cierto tanto para el caso de Colombia como para el de los demás países que mencionamos.

En primer lugar, la mayoría de regímenes están establecidos en una mezcla de leyes y decretos, por lo que la retención de datos no siempre ha sido materia de discusión en los congresos. En cuanto a la legalidad, la legislación colombiana usa términos particularmente ambiguos y las autoridades que pueden acceder a los datos retenidos. Pero el principal problema no es la legalidad, pues bien puede aprobarse una ley que viole derechos fundamentales. El problema es la falta de objetivos legítimos y de ahí que la retención de datos no sea una medida necesaria y proporcional. A excepción de México, ningún otro país define qué es la seguridad nacional, que es el objetivo que se persigue cuando la retención de datos se establece como una herramienta para labores de inteligencia. Colombia, como los demás países, simplemente evoca este objetivo sin desarrollarlo ni limitarlo. Por tanto, si el objetivo que busca la medida no es legítimo, no puede hablarse de necesidad y proporcionalidad pues estos requisitos existen en relación con ese objetivo. Por naturaleza la orden de retener datos es automática y no pasa por ningún control judicial, de ahí que tampoco esté a la altura de los estándares internacionales de los que hemos hablado. Esta situación, en combinación con la falta de notificación a las personas usuarias y la escasa implementación de obligaciones de transparencia hace que el uso de la retención de datos aún esté en la sombra y por tanto, la ciudadanía carezca de datos para determinar la utilidad de esta medida.

La retención de datos debe ser una de las técnicas de vigilancia más usada en la región, o al menos de las primeras herramientas utilizadas por las autoridades, a juzgar por la forma como las legislaciones se han esparcido para legalizarla. De los 5 países que

analizamos, 4 de ellos han legislado esta técnica y no son las únicas legislaciones de este tipo en la región. Países como Honduras y Chile también cuentan con normas de retención de datos y con un análisis detallado, seguramente, emergerán muchas más.

Sin embargo, que exista legislación que reglamente el uso de la retención de datos, por sí solo, no es garantía de protección a los derechos humanos. Una legislación de ese tipo debe cumplir con una serie de condiciones para que la práctica sea legítima. Ninguna de las legislaciones que vimos pasa el análisis. Las leyes sobre retención de datos de Perú, Colombia, México y Brasil son demasiado permisivas, amplias y tan poco garantes que no es posible confiar en ellas para tener un marco legal protector y respetuoso de los derechos humanos de su ciudadanía, como quedó demostrado en este documento. De otra parte, la legislación que hubo en Argentina fue declarada inconstitucional, precisamente, después de que se estableciera que no era clara ni proporcional.

Es preocupante que, en materia de técnicas de vigilancia, se esté privilegiando una mirada esencialmente instrumental de la tecnología, que no cuestiona su verdadera utilidad. Si se hiciera una evaluación de este tipo, el carácter residual de la retención de datos frente a otras técnicas dirigidas y menos invasivas sería evidente. El marco jurídico que ofrece la CIDH y otros análisis como el que articulan los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* deben servir para promover legislaciones que ofrezcan verdaderas garantías para la ciudadanía y mejoren la seguridad jurídica sobre la que se deben soportar las autoridades para hacer su trabajo.

Sería recomendable que tanto Colombia como los demás países analizados demuestren su compromiso fuerte con la protección de derechos humanos y desmonten la retención de datos que existe actualmente. La Unión Europea y Argentina han mostrado que la retención de datos es una medida de vigilancia masiva que pone bajo sospecha a toda la ciudadanía y afecta la intimidad de sus comunicaciones, de ahí que no sea ni necesaria ni proporcional para defender objetivos como la seguridad nacional o los intereses de los procedimientos penales. Si sectores de la sociedad o el gobierno consideran que la retención de datos puede establecerse sin violar derechos fundamentales, debería abrirse el debate para discutir cada uno de los aspectos que hemos señalado acá como falencias de la retención de datos. Hasta tanto, la retención de datos como se presenta actualmente debe ser considerada como una medida ilegítima de vigilancia ciudadana.

NOTAS

1. CIDH (2013). *Libertad de expresión e internet*. OEA/Ser.L/V/II.149 Doc.50, Capítulo IV, párr. 154.
2. Perú: Morachimo, M. Vigilancia Estatal de las Comunicaciones y Derechos Fundamentales en Perú (Octubre, 2015). Electronic Frontier Foundation e Hiperderecho. Recuperado de: https://www.eff.org/files/2015/11/24/peru-es-final.pdf
3. García, L. Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México (Octubre, 2015). Electronic Frontier Foundation y Red en Defensa de los Derechos Digitales. Recuperado de: https://www.eff.org/files/2015/11/24/mexico-es-final.pdf
4. Antonialli, D. y de Souza Abreu, J. State Surveillance of Communications in Brazil and the Protection of Fundamental Rights (Septiembre, 2015). Recuperado de https://en.necessaryandproportionate.org/files/2015/12/03/brazil-en-dec2015.pdf
5. Rivera, J. y Rodríguez, K. Vigilancia de las comunicaciones por la autoridad y protección de los derechos fundamentales en Colombia (Mayo, 2015) Recuperado de: https://www.eff.org/files/2015/05/19/colombia-principios-may-14.pdf
6. Ferrari, V. y Schnidrig, D. Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina (Octubre, 2015) Recuperado de: https://en.necessaryandproportionate.org/files/2015/12/04/argentina-sp-dec2015.pdf
7. Castañeda, J. (2015). Cuando el Estado hackea. Recuperado de: https://karisma.org.co/wp-content/uploads/2015/12/CUANDO-EL-ESTADO-HACKEA-D.pdf
8. Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA (2015, 21 de julio). Comunicado de prensa sobre la adquisición e implementación de programas de vigilancia por parte de Estados del hemisferio. Recuperado de http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=998&lID=2.

9. *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*. Recuperado de https://es.necessaryandproportionate.org/text.

10. CIDH (2013). *Libertad de expresión e internet*. OEA/Ser.L/V/II.149 Doc.50, Capítulo IV, párr. 55.

11. Solove, D.J. (2004). *The digital person technology and privacy in the information age*. New York, U.S.: New York University Press.

12. Schneier, B. (2015). Data and Goliath: the hidden battles to collect your data and control your world. New York, U.S.: W. W. Norton.

13. Kerr, I.R., Gilbert, D. & McGill, J. (2006). The medium and the message: personal privacy and the forced marriage of police and telecommunications providers.*Criminal Law Quarterly*, 51(4).

14. Electronic Frontier Foundation & American Civil Liberties Union Brief *Amicus Curiae* en Kalyman v. Obama,20 de agosto de 2014. Disponible en https://www.eff.org/document/eff-and-aclu-amicus-brief-klayman.

15. Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (2014). *El derecho a la privacidad en la era digital*. A/HRC/27/37, parr. 19.

16. Naciones Unidas. Asamblea General. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue. A/HRC/23/40, párr. 148

17. *Supra* (nota 1), Capítulo IV, párr. 58.

18. Ministerio de Planificación Federal, Inversión Pública y Servicios (2013, 1 de julio). Resolución No. 5. Recuperado de http://infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/216915/norma.htm.

19. Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal (2005, 29 de noviembre). *Halabi v. Estado Nacional*.

20. Decreto No. 1704 de 2012, artículos 4 y 5.

21. Ley No. 1621 de 2013, artículo 44.

22. Ley No. 27.336 (2002)

23. Decreto Legislativo No.1182, primera y segunda disposición final complementaria.

24. Resolución No. 426 de 2005, artículo 22.

25. Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) Artículo 190 III.

26. Decreto No. 1704 de 2012, artículos 4 y 5.

27. En Colombia, son agencias de inteligencia: la Dirección Nacional de Inteligencia, la Unidad de Información y Análisis Financiero, la Dirección de Inteligencia de la Policía y las correspondientes jefaturas dentro del Comando General de las Fuerzas Militares, el Ejército Nacional, la Armada Nacional y la Fuerza Aérea. *Véase* el Decreto No. 857 de 2014.
28. Decreto Legislativo No. 1182. Artículos 3 y 4.
29. Código Procesal Penal, artículo 230, numerales 1 y 4.
30. CIDH, *op. cit.* (nota 1), Capítulo IV, párr. 157; CIDH (2009). *Informe anual de la Relatoría Especial para la Libertad de Expresión.* OEA/Ser.L/V/II Doc.51, Capítulo III, párr. 76.
31. *Supra*, Capítulo III, párr.77-80.
32. *Supra*, Capítulo III, párr. 81-83.
33. *Supra* (nota 1), Capítulo IV, párr. 60 y 157.
34. *Supra* (nota 39), Capítulo III, párr. 85-87 & *Supra* (nota 1), Capítulo IV, párr. 64, 160 y 162.
35. *Supra* (nota 39), Capítulo III, párr. 88.
36. *Supra* (nota 1), Capítulo IV, párr. 90.
37. Relator Especial de las Naciones Unidas para la protección y promoción del derecho a la libertad de opinión y de expresión & Relatora Especial para la libertad de expresión de la CIDH de la OEA (2013, 21 de junio). *Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión*. Punto 9.
38. Tribunal de Justicia de la Unión Europea (2014, 8 de abril). *Sentencia Digital Rights Ireland*, párr. 56, 57, 59 y 63.
39. Breyer, P. (2005). Telecommunications data retention and human rights: the compatibility of blanket traffic data retention with the ECHR. *European Law Journal*, 11(3).
40. *Supra* (nota 1), Capítulo IV, párr. 65.
41. *Supra* (nota 1), Capítulo IV, párr. 165.
42. *Marc Civil*. Ley No.12.965 de 2014, artículos 10(3), 13(5), 15(3) y 22.
43. *Supra* (nota 1), Capítulo IV, párr. 164.
44. *Supra* (nota 1), Capítulo IV, párr. 168.
45. *Supra* (nota 1), Capítulo IV, párr. 168 y 169.