Vigilancia de las comunicaciones en Colombia

El abismo entre la capacidad tecnológica y los controles legales

Carlos Cortés Castillo

DOCUMENTOS 18

Dejusticia
derecho · justicia · sociedad

DOCUMENTOS 18

Vigilancia de las comunicaciones en Colombia

El abismo entre la capacidad tecnológica y los controles legales

Carlos Cortés Castillo

Carlos Cortés Castillo Abogado de la Universidad de los Andes (Colombia) y magíster en Gobernanza de Medios del *London School of Economics* (Inglaterra). Sus campos de trabajo son: libertad de expresión, medios de comunicación, medios digitales, *Internet*. Colaboró con Dejusticia dentro del proyecto financiado por Privacy International para facilitar la implementación de actividades relacionadas con la vigilancia y la libertad.

Dejusticia
derecho · justicia · sociedad

Documentos Dejusticia 18
VIGILANCIA DE LAS COMUNICACIONES EN COLOMBIA
El abismo entre la capacidad tecnológica y los controles legales

Este trabajo se desarrolló gracias al apoyo de
Privacy International e *International Development Research Centre (IDRC).*

ISBN: 978-958-58464-2-5 versión impresa
978-958-58464-1-8 versión digital

Centro de Estudios de Derecho, Justicia y Sociedad, Dejusticia
Carrera 24 Nº 34-61, Bogotá, D.C.
Teléfono: (57 1) 608 3605
Correo electrónico: info@dejusticia.org
http://www.dejusticia.org

Revisión de textos: Emma Ariza
Preprensa: Marta Rojas
Cubierta: Alejandro Ospina
Impreso por Ediciones Antropos

Bogotá, julio de 2014

Contenido

Agradecimientos

A Vivian Newman,
por ayudarme a estructurar este documento.

A los investigadores de Dejusticia,
por los comentarios a la primera versión.

A Juan Diego Castañeda,
por su apoyo en la fase de investigación.

Introducción

El año pasado, los medios de comunicación revelaron que la Policía Nacional pondría en operación la Plataforma Única de Monitoreo y Análisis (PUMA), a través de la cual se podría interceptar "lo que se hable, escriba o envíe desde correos electrónicos, Facebook, Twitter, Line, Viber, Skype y, en definitiva, todo tipo de comunicación que se realice a través de Internet".[1] Más recientemente, en febrero pasado, la revista *Semana* denunció que la inteligencia militar revisaba los correos electrónicos y chats de los negociadores de paz en La Habana, Cuba.[2]

En ambos casos, el Gobierno le dio un giro a la noticia. En el primero, PUMA no era nada más que el reemplazo de otro sistema, que de cualquier forma funcionaría con los debidos controles legales.[3] En el segundo caso, el Presidente rápidamente anunció una comisión para definir la política de ciberseguridad y ciberdefensa de la nación.[4]

Las preguntas de fondo, sin embargo, no fueron resueltas. ¿Cuál era, a la postre, la capacidad técnica de PUMA? ¿Es posible revisar los correos

1 *El Tiempo.* 2013. "Policía podrá interceptar Facebook, Twitter y Skype en Colombia", 22 de junio. Recuperado de: http://www.eltiempo.com/justicia/ARTICULO-WEB-NEW_NOTA_INTERIOR-12890198.html (consultado el 5 de abril de 2014).

2 Cfr. Revista *Semana.* 2014. "Chuzadas: así fue la historia", 8 de febrero. Recuperado de: http://www.semana.com/nacion/articulo/chuzadas-asi-fue-la-historia/376548-3 (consultado el 5 de abril de 2014).

3 Revista *Semana.* 2013. "La polémica que se desató por PUMA", 29 de junio. Recuperado de: http://www.semana.com/nacion/articulo/la-polemica-desato-puma/349109-3 (consultado el 5 de abril de 2014).

4 *Enter.co.* 2014. "Así construye Colombia su política de ciberseguridad y ciberdefensa", 31 de marzo. Recuperado de: http://www.enter.co/chips-bits/seguridad/ciberdefensa-colombia-politica/ (consultado el 5 de abril de 2014).

electrónicos de cualquier persona? ¿Puede la inteligencia militar revisar los chats de alguien? ¿Es lo mismo interceptar un teléfono que Internet?

A pesar de que en Colombia cada tanto se conoce algún escándalo relacionado con inteligencia estatal, nunca queda claro cómo funciona en la práctica y qué controles existen para su ejercicio. Entretanto, pasa el tiempo y los esquemas de vigilancia se sofistican a la par con nuestros teléfonos móviles y computadores.

Un teléfono analógico de disco es tan obsoleto como los cables "cocodrilo" que se usan para interceptar sus llamadas. No obstante, mientras el mercado facilita el proceso de obsolescencia y la incorporación de nuevas tecnologías masivas, poco o nada dice sobre los dispositivos que en paralelo se desarrollan para vigilar al individuo.

Los cambios tecnológicos suelen alterar presunciones largamente establecidas sobre el alcance de determinados derechos. La privacidad, sin duda, es el derecho que más tensiones enfrenta en el entorno digital. A pesar de esto, en la regulación y en la jurisprudencia subsisten lagunas sobre cómo la tecnología impacta el ejercicio de derechos fundamentales.

Los casos de PUMA y del café Internet para hacer inteligencia militar llegan poco después de que Colombia adoptara una Ley de Inteligencia que, en teoría, evitaría las irregularidades de antes y se pondría a tono con la vigilancia moderna. Pero, ¿es ese realmente el caso? ¿Tenemos una regulación para preservar la seguridad nacional sin comprometer la privacidad y la libertad de expresión, entre otros?

El objetivo de este documento es examinar el marco legal y jurisprudencial colombiano sobre vigilancia de comunicaciones, a la luz de las capacidades tecnológicas de hoy. Dicho a manera de hipótesis, el propósito es mostrar cómo la regulación y la jurisprudencia en materia de inteligencia no se ocupan de interpretar los esquemas de vigilancia actuales para mantener vigentes los derechos que resultan afectados.

Para desarrollar este objetivo, abordamos algunos puntos –escogidos con cierto nivel de arbitrariedad– de la Ley de Inteligencia: interceptación de comunicaciones, monitoreo del espectro electromagnético y acceso a datos de usuarios. Este último tema, que tomado de manera independiente merecería un estudio aparte, se desarrolla como complemento de los dos primeros.

El documento está divido de la siguiente forma: el primer capítulo explica, desde el punto de vista técnico, cuáles son las tecnologías para comunicarnos y cuáles existen para vigilarnos. El segundo capítulo desarrolla el marco legal sobre vigilancia de las comunicaciones. El tercero ofrece un panorama general comparado frente a la interceptación de las comunicaciones en particular. Finalmente, el cuarto capítulo analiza lo hasta allí planteado para ofrecer algunas conclusiones.

Tecnología para comunicarnos y vigilarnos

La interceptación y el monitoreo de comunicaciones están inexorablemente ligados a las formas de comunicarse. Con las cartas y el servicio postal apareció la revisión de sobres y paquetes; con el telégrafo llegaron los lectores de telegramas; con el teléfono vinieron las pinzas para interceptar cables (Hosein y Wilson 2013: 1071-1104). Bien sea de manera directa o a través de terceros, los gobiernos siempre han tenido alguna expectativa de control sobre las palabras que intercambian sus ciudadanos.

La telefonía móvil, el Internet y la tecnología digital en general, no son la excepción a esa regla. Así como las comunicaciones de hoy son móviles, globales e instantáneas, los esquemas de vigilancia subyacentes se hacen desde cualquier parte y en tiempo real. Con la misma facilidad que dos personas hablan, un tercero observa o escucha.

En este primer capítulo se explicará de manera general el trasfondo técnico de la telefonía analógica, el Internet y la telefonía móvil. A partir de esto, se describirá la tecnología disponible para interceptar y monitorear las comunicaciones modernas. Como veremos, son diversos los cambios tecnológicos que determinan y, a la vez, obligan a reconfigurar los esquemas de vigilancia.

Del teléfono de disco al WhatsApp

Conmutación de circuitos y conmutación de paquetes

La red telefónica tradicional se desarrolló a imagen y semejanza de la red ferroviaria. De hecho, en muchas partes del mundo, los cables del telégrafo –el antecesor del teléfono– iban a la par de los rieles, y las oficinas de este servicio quedaban en las estaciones de tren. Con el tiempo, esta red de comunicaciones fue evolucionando de manera descentralizada, pero jerárquica, siguiendo los patrones de ciudades y poblaciones: un grupo

de habitantes conectados a una central telefónica, y una serie de centrales conectadas entre sí (Landau 2010).

Las primeras llamadas se hacían a través de una operadora (generalmente esta labor estaba a cargo de una mujer), que se encargaba de conectar los extremos de cada red mediante conmutadores (*switches*) manuales. Para ese efecto, el número telefónico le indicaba la ciudad, la central telefónica y el teléfono de destino. Con la llegada de la conmutación telefónica automática –inventada a finales del siglo XIX por el norteamericano Alan Strowger–, el proceso se agilizó y las redes comenzaron a expandirse.

La red pública telefónica destina un canal exclusivo para la comunicación entre dos extremos. Esta metodología se conoce como conmutación de circuitos o *circuit switching*. En otras palabras, cuando una persona llama a otra desde su casa, la línea solo puede transmitir esa conversación. La voz viaja como impulsos eléctricos que emplean toda la capacidad del cable. Incluso si hay silencio, el canal debe estar dispuesto para esa comunicación (Farahmand y Zhang 2007).

A medida que la red telefónica fue interconectándose entre proveedores, ciudades y países, empezó a tener redundancias: había varios caminos posibles para llegar del punto A al punto B. En esas condiciones, era posible establecer varias rutas independientes entre distintos extremos de la red. Esa idea fue el gen de Internet (Wu 2010).

Internet no es otra cosa que una red jerárquica de computadores. El computador A está conectado a un *router* (el aparato que parpadea al lado del computador); el *router* está conectado al proveedor del servicio (Telmex, por ejemplo); el proveedor del servicio está conectado a un servidor más grande, y este a un servidor central –conocido como espina dorsal o *backbone*–. La ruta es la misma desde la espina dorsal hasta el computador B, pero es posible que los proveedores de servicio de A y de B estén conectados entre sí, con lo cual una conexión entre A y B no debe pasar necesariamente por el punto más alto de la red. Es decir: un correo electrónico de pablo@telmex.com.co a sandra@etb.com.co puede ir simplemente del computador de Pablo, a Telmex, de Telmex a ETB, y de ETB al computador de Sandra.

Para poder aprovechar la capacidad de la red y establecer conexiones simultáneas, Internet funciona con una metodología distinta a la conmutación de circuitos, conocida como *conmutación de paquetes* (*packet switching*). Esta metodología divide los datos en paquetes en el punto de origen y los transmite, en distinto orden y por distintas vías, hasta su destino, donde se rearman y adquieren el sentido original. Todo el proceso sigue un protocolo de conexión y transporte conocido como TCP/IP.

La conmutación de paquetes se complementa con un principio de estratificación o de capas, también conocido como *modelo de interconexión de sistemas abiertos*. Para los fines de este documento, basta con entender que cada paquete de datos contiene una serie de capas: las más superficiales con la información necesaria para transportar y rearmar el paquete en su destino, y las más profundas con una parte de los datos objeto de la transmisión. En este sistema, los *routers* de la red tienen la misión de llevar los paquetes a su destino, para lo cual solo necesitan "ver" las capas superficiales de estos (tanto como si solo tuvieran que ver la dirección escrita en un sobre). De lo demás se encargan las terminales finales (el computador personal, por ejemplo). Es por esto que Internet se conoce como una "red tonta" con inteligencia en los extremos, y es este diseño el que sustenta el concepto de neutralidad de la red.[1]

Ilustremos este proceso con un ejemplo: cuando Andrés le envía un correo a María, el computador de Andrés se encarga de dividir los datos en paquetes y enviarlos por la red. A través de esta viajan –dirigidos por los *routers*– en cualquier orden y por distintas vías. Si en el tránsito de un computador a otro se "observara" alguno de estos paquetes individualmente, no se accedería a un mensaje o a una conversación inteligible, como sí sucede en el sistema telefónico analógico. Solo se tendría acceso a una porción de los datos. En el destino, el computador de María se encarga de rearmar los paquetes para que el mensaje aparezca como Andrés lo escribió. Gracias a la información de cada paquete, el computador de María sabe en qué orden debe integrarse con los demás y qué aplicación está en capacidad de "leerlos".

Espectro radioeléctrico y servicios móviles

La telefonía celular y los servicios móviles funcionan de otra forma. Para empezar, en vez de transportar los datos a través de cables, estos servicios utilizan el espectro electromagnético, que es el espacio que abarca todos los conjuntos de ondas electromagnéticas. El espectro radioeléctrico, en particular, se refiere a la franja apta para servicios de telecomunicaciones dentro del espectro electromagnético.[2]

1 Para una explicación más detallada de la arquitectura de Internet, ver Cortés (2014a y 2014b)

2 Este capítulo se basa mayoritariamente en Poole (2006).

Las ondas electromagnéticas, como las olas del mar, son ondulantes y transmiten energía, pero a diferencia de aquellas, estas "viajan" por el aire a la velocidad de la luz. El carácter ondulante de la onda es el producto de la vibración de las partículas cargadas, que tienen propiedades magnéticas y eléctricas. Si la cantidad de energía es baja, la distancia entre cresta y cresta en la onda es larga, y, por lo tanto, decimos que tiene una frecuencia baja (las ondas radiales, por ejemplo, tienen esta característica). Al contrario, si la energía es mayor, la distancia entre cada cresta es muy corta y decimos que la frecuencia de la onda es alta (es el caso de los rayos X o Gamma). Cuanto más larga sea la onda, mayor será su penetración.

Para prestar los servicios móviles, el Gobierno les asigna a los operadores –a través de distintos mecanismos– una o varias frecuencias del espectro radioeléctrico. Estas frecuencias son la "autopista" por donde se transmiten las ondas de voz y datos. Teniendo en cuenta el carácter limitado de esa porción de espectro, y, a la vez, su capacidad infinita de reutilización, los operadores usan estaciones transmisoras-receptoras (o estaciones base) para llevar los datos de un lado a otro. Estas estaciones son fijas y lucen como una antena.

Cuando hacemos una llamada desde nuestro celular o enviamos un mensaje de texto, la estación base más fuerte en el área –con mejor señal– recibe los datos de nuestro dispositivo y los transmite a la estación base más fuerte para el receptor. Esta última, a su vez, transmite los datos al destinatario.[3] Cada estación base cubre un área limitada. Supongamos que una estación ubicada en la Calle 100, en Bogotá, cubre entre las calles 90 y 110 y las carreras 1 a 25. Más allá de esa circunferencia, la señal se perderá (la llamada se cae) o habrá interferencia.

Para resolver ese problema, los operadores instalan varias estaciones y dividen un área en múltiples regiones pequeñas, con lo cual es posible reutilizar más eficientemente el espectro, garantizar el servicio y atender una mayor demanda. Estas regiones se conocen como celdas. Dependiendo de la cantidad de celdas, entre otros, es posible transmitir más datos y en mejores condiciones. Por esto, una ciudad requiere una red más densa que en el campo, lo que significa una mayor infraestructura.

3 La transmisión de voz y datos en los servicios móviles sigue una metodología similar a la conmutación de paquetes en el Internet fijo. Esto es, por las ondas radioeléctricas no "viaja" la voz como tal, sino una serie de paquetes con porciones de datos que se rearman en el destino.

El teléfono móvil es, a la larga, un punto que siempre está en el radar del operador. Cada vez que prendemos nuestro celular o a medida que nos movemos con él, la estación base más fuerte se conecta con el dispositivo para determinar su identidad y legitimidad dentro del sistema. Dicha autenticación se logra a través del IMEI (*International Mobile Equipment Identity*), un serial de quince dígitos que permite identificar el equipo y asociarlo a un suscriptor y un plan determinado. (Esto además evita, en teoría, que un celular robado entre a la red).

En otras palabras, para que nuestro celular funcione, el prestador del servicio necesita saber permanentemente, y con algún nivel de precisión, en qué zona estamos. Triangulando los datos de varias estaciones, un operador en una zona urbana –que, recordemos, tiene una infraestructura más próxima al usuario que en el campo– puede llegar a determinar nuestra ubicación en un radio de menos de 50 metros (Pell y Soghoian 2012: 117).

Datos de datos

La ubicación permanente de nuestro teléfono móvil –o sea, nuestra ubicación– se almacena en los registros históricos del operador del servicio junto con los datos de llamadas realizadas y recibidas, su duración y –cuando se tiene el servicio de Internet móvil– las páginas visitadas y aplicaciones usadas.

Los teléfonos inteligentes o *smartphones* cuentan, además, con tecnologías complementarias que generan datos y eventualmente determinan la ubicación del usuario. Por una parte, estos dispositivos pueden conectarse a redes inalámbricas (*wi-fi*), con las cuales comparten información para acceder a Internet. Por la otra, tienen sistemas de posicionamiento global (GPS), cuya funcionalidad es la esencia de servicios basados en localización (*location based services*) como Maps, Find My Friends o Foursquare – aplicaciones que georreferencian al usuario o que, a partir de su ubicación, prestan un servicio.

Estos datos no contienen en sí mismos la conversación, el mensaje o el objeto de la comunicación, sino alguna información sobre su contenido. Es lo que se conoce como metadatos: datos que describen otros datos (Mayer-Schönberger y Cukier 2013). Un número telefónico o la duración de una llamada no dice de qué se trató la llamada, ni la dirección de un correo electrónico o la cantidad de mensajes enviados equivalen al texto. Sin embargo, unos y otros proporcionan información valiosa sobre el fondo de la comunicación. Más aún si todos estos datos pueden indexarse y analizarse.

Además de estos rastros digitales que dejan nuestras comunicaciones, las aplicaciones y los servicios que usamos desde nuestros teléfonos móviles y computadores –desde el Internet fijo y el Internet móvil– son auténticos expedientes personales: en Gmail están nuestros correos electrónicos de los últimos años; en Twitter hay decenas de mensajes directos; en Flickr hay fotos y videos, y en WhatsApp hay conversaciones anodinas y trascendentales. Estos ya no son metadatos, sino datos que se alojan en los servidores de quien administra la aplicación o la red social que usamos.

Formas modernas de vigilancia

La interceptación de una llamada hecha a través de la red telefónica conmutada es un proceso relativamente simple: en cualquier punto de la comunicación –en uno de los teléfonos, en algún punto del cable, en las cajas de interconexión, en la central telefónica o en los postes– se ubica un dispositivo que envía las señales para escuchar la conversación o para efectuar una grabación (Landau 2010).

A estas alturas parece claro que ese procedimiento no funcionaría para interceptar una conversación móvil o un intercambio de correos electrónicos. No obstante, que haya distintas maneras de vigilar las comunicaciones modernas no implica que haya fronteras claras entre las formas de hacerlo y las plataformas aplicables. La vigilancia sigue, más bien, un paradigma de acceso: ¿cómo accedemos a una comunicación?, ¿por dónde entramos?, ¿cómo obtenemos lo que necesitamos? Lo que evidenciamos hoy es la expansión de tecnologías de vigilancia cuya característica principal es la ubicuidad y la capacidad para integrarse a las arquitecturas modernas de comunicaciones (Marquis-Boire et ál. 2013a).

Hosein y Wilson identifican tres tipos de tecnologías para la vigilancia de las comunicaciones, desarrolladas e implementadas alrededor del mundo: i) las ofensivas de uso dirigido, ii) las dirigidas y semidirigidas para comunicaciones móviles, y iii) las de vigilancia masiva en Internet (Hosein y Wilson 2013: 1071-1104). Estas categorías ofrecen, sobre todo, una orientación metodológica.

Tecnologías de uso dirigido

Las tecnologías ofensivas de uso dirigido permiten obviar la acción previa de incautar un equipo para su inspección. Sin el conocimiento del propietario del equipo y a distancia, el agente usa "puertas traseras" (*backdoors*) del sistema o de un programa en particular, o las crea con un software maligno o *troyano*. De ahí el adjetivo de "ofensivo" de esta tecnología.

Los programadores suelen incluir "puertas traseras" en los sistemas y aplicaciones para que se pueda ingresar a estos cuando presentan errores o daños, o cuando no hay acceso por la entrada principal –es decir, usando el nombre de usuario y la contraseña–. Se trata, en esencia, de un privilegio del creador o administrador de la aplicación, algunas veces requerido por mandato legal para facilitar, precisamente, labores de inteligencia. Las puertas traseras no son malas per se, pero pueden existir y operarse sin que el usuario esté al tanto. Peor aún, pueden crearse instalando un software maligno o *troyano* en el dispositivo.

Para abrir o crear la puerta trasera es necesario que el agente adquiera el control de la máquina que quiere vigilar. Si hubo contacto físico con el computador, simplemente hay que instalar el *troyano* –con una USB o un CD–. Y si es a distancia, es necesario engañar al usuario para que instale el software maligno pensando que se trata de otra cosa.

En abril del año pasado, la Fundación Mozilla informó que la empresa alemana Gamma Internacional había creado una falsa actualización del navegador Firefox para instalar *troyanos* con fines de vigilancia. Así, el usuario descargaba un archivo con la convicción de que estaba instalando la última versión del programa cuando, en realidad, estaba activando una puerta trasera en su equipo. Más allá de si la práctica era legal, Mozilla denunció que se estaba afectando su producto y su marca (Fowler 2013).

El Citizen Lab de la Universidad de Toronto ha documentado casos similares en el contexto de la Primavera Árabe. En Bahréin, por ejemplo, los activistas fueron objeto de ataques con *troyanos* anexos a correos electrónicos. El sujeto simplemente recibía un correo con el nombre de una periodista conocida que enviaba una serie de fotos sobre unos activistas arrestados. En efecto, había unas fotos anexas, pero al descargarlas se instalaba también el software maligno en el equipo. La cuenta de la periodista, al parecer, era falsa (Marquis-Boire et ál. 2013a).

Una vez se abre una puerta trasera y se instala un *troyano,* el agente adquiere control del computador –suponiendo, como es común, que está conectado a Internet– tanto como si hubiera entrado a nuestra casa: puede extraer y acumular datos (*data harvesting*), descargar archivos, extraer nombres de usuarios y contraseñas, prender la cámara del equipo, controlar el teclado y monitorear Skype, entre otros. Si se trata de un celular, puede incluso activar una "llamada silenciosa", con lo cual el teléfono se vuelve un micrófono.

Diversas compañías desarrollan y comercializan este tipo de programas. La actualización falsa de Mozilla, en particular, hace parte de un producto llamado *FinFisher,* usado en al menos 25 países (México, entre ellos). *FinFisher* se comercializa como una "solución de monitoreo remoto" que recoge información del computador infectado y la envía a un servidor (Marquis-Boire et ál. 2013b).

Tecnologías dirigidas y semidirigidas para comunicaciones móviles

Las tecnologías de uso dirigido y semidirigido de teléfonos móviles permiten monitorear activamente las comunicaciones móviles en terreno. Según como se use –y como su nombre lo indica– pueden estar dirigidas a un sujeto en particular o indiscriminadamente contra todas las personas que tengan teléfonos móviles en la zona.

El dispositivo más común es el simulador de estación celular, conocido como *receptor IMSI* (por su sigla en inglés, identidad internacional del suscriptor móvil). En el mercado se conoce por la marca Mantarraya o *Stingray,* de la empresa norteamericana Harris Corporation; para septiembre de 2013, la versión más avanzada costaba unos 135 mil dólares. Al ser un dispositivo móvil que no requiere conectarse físicamente a la red para operar –cabe fácilmente en el baúl de un carro pequeño–, es imposible que el usuario lo detecte y muy difícil que los propios operadores móviles lo descubran (Strobel 2007).

La función del *Stingray* es hacerse pasar por la estación celular con mejor señal para el teléfono móvil del sujeto (recordemos que los teléfonos móviles están conectándose constantemente con la estación que emita la mejor señal en la zona) para identificar su IMSI. El IMSI, como su nombre lo indica, es la identidad del dispositivo en la red; siempre está asociado a un número celular y, en últimas, a un suscriptor.

"Al suplantar la estación base, todos los teléfonos móviles de esa red en esa área se conectarán con el dispositivo de monitoreo en vez de conectarse con la red legítima. El dispositivo puede entonces identificar todos los teléfonos al alcance. En una versión más avanza de implementación, también puede lograr un acceso directo a los contenidos de las comunicaciones y los metadatos al enrutar llamadas a través de la estación base", explican Hosein y Wilson (2013: 1081).

En otras palabras, este dispositivo puede identificar uno o varios celulares de las personas que se encuentran en un lugar público o privado –una manifestación, una reunión a puerta cerrada–. Basta con cruzar los IMEI con los números de teléfono y los titulares de las cuentas, información esta última que los operadores de las redes están usualmente obligados a suministrar. En la modalidad más sofisticada, un *Stingray* puede intermediar una transmisión individual para acceder a todos los datos que por allí pasen.

Otro *receptor IMSI* disponible en el mercado es el Gossamer, un dispositivo portátil –del tamaño de un celular de los años ochenta– que además de ubicar celulares en una zona a través del IMEI, puede bloquear el teléfono del blanco para que no haga ni reciba llamadas (estos ataques se conocen en inglés como *denial of service attack*). Para el año 2013 tenía un costo comercial de unos 20 mil dólares (Gallagher 2013).

Tecnologías de vigilancia masiva en la red

Por último, están las tecnologías de vigilancia masiva en la red, cuyo propósito es recolectar grandes cantidades de información para análisis posterior. El mejor ejemplo de este tipo de vigilancia se dio con el escándalo "Prisma", destapado en 2013 por *The Guardian* y otros medios de comunicación.

Según la información divulgada por el excontratista de la CIA Edward Snowden, la Agencia de Seguridad Nacional de Estados Unidos había tenido acceso a las bases de datos de Google, Facebook, Apple y otros proveedores de servicios de Internet. Historiales de búsqueda, correos electrónicos, archivos y *chats*, entre otros, estaban ahora en poder de la inteligencia norteamericana.[4]

En términos generales, hay dos vías para acceder a esta información: bien sea con la colaboración del proveedor del servicio o, de manera subrepticia, abriendo una puerta trasera u observando el tráfico que pasa por algún punto de la red. No son opciones excluyentes. Los informes periodísticos apuntan a una combinación entre la colaboración de los intermediarios (Google, Facebook, Yahoo, etc.) y el monitoreo de los "cables y tubos" de la red.[5]

4 Cfr. *The Guardian*, "NSA Prism program taps in to user data of Apple, Google and others", 7 de junio de 2013. Recuperado de: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (consultado el 19 de marzo de 2014).

5 Cfr. *The Guardian,* "US tech giants knew of NSA data collection, agency's top lawyer insists". Recuperado de: http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de (consultado el 19 de marzo de 2014). Ver también *The Atlantic*, "The

En el primer caso, los prestadores de servicios de Internet y las agencias estatales habrían tenido –o tienen– algún mecanismo para compartir información. Bien puede ser una entrega permanente de información o, quizá más probable, una puerta trasera creada por las empresas para que los agentes puedan consultar fácilmente la información que necesiten.

En el segundo escenario, las agencias del Gobierno habrían usado –o usan– tecnología para monitorear el tráfico en puntos estratégicos de la red. Como vimos, Internet es una red jerárquica con servidores locales, puntos de interconexión, espinas dorsales y cables submarinos a la entrada de los países. Dependiendo de donde se ponga el dispositivo para monitorear el tráfico, habrá más o menos datos para analizar. De una u otra forma, este trabajo es muy complejo, debido a la inconmensurable cantidad de datos que pasan por un cable, y requiere equipos que permitan analizar el tráfico en busca de paquetes de datos con información o palabras clave.

Una de las tecnologías empleadas para este fin es la *inspección profunda de paquete* (*deep packet inspection*). Como ya se explicó, los datos viajan por la red divididos en paquetes, los cuales, a su vez, están divididos por capas; las capas superficiales contienen la información básica que identifica el paquete, mientras las profundas incluyen los datos objeto de la transmisión. Mediante una "caja negra", que debe estar conectada a algún punto de la red, el tráfico se analiza, se seleccionan paquetes y se examinan sus capas profundas para identificar contenidos determinados.[6]

Las capas más superficiales de los paquetes contienen metadatos relevantes, como el correo electrónico de un destinatario, el asunto de un mensaje o la aplicación empleada. Así, aunque los contenidos más profundos no se observen, ya existe una información útil para copiar, indexar y analizar. Y aunque hay tecnologías para codificar estos datos de manera que solo las partes autorizadas accedan a ellos –o sea, tecnologías de encriptación–, en general las redes sociales y los servicios en línea no cuentan con una seguridad demasiado sofisticada.

Algunas de las tecnologías referidas en este capítulo no están diseñadas exclusivamente para vigilar la actividad de los usuarios en Internet. También sirven para monitorear el funcionamiento correcto de un sistema, mejorar la calidad del servicio de una conexión o prevenir, precisamente, el uso de software maligno. Por esa razón, están al alcance de proveedores de servicios y operadores de redes, lo cual hace aún más difícil el ejercicio de cualquier control.

Vigilancia de las comunicaciones en Colombia

El régimen legal colombiano diferencia la interceptación de comunicaciones del monitoreo del espectro electromagnético. Mientras la primera actividad se enmarca en investigaciones penales concretas, a partir de una noticia criminal y con el propósito de buscar pruebas para identificar a los autores de un delito, la segunda hace parte de las actividades de inteligencia del Estado; no se hace con el fin de perseguir a una persona en concreto, sino con el objetivo de prevenir usos ilegítimos del espectro.[7]

En este capítulo se explican ambos conceptos desde la jurisprudencia constitucional, el Código Penal y la Ley de Inteligencia, recientemente expedida por el Congreso y avalada por la Corte Constitucional. Por último, se hace referencia a las facultades que, tanto en materia de investigación judicial como inteligencia, tienen las autoridades para acceder a los datos de los usuarios que se encuentran en manos de los proveedores de redes y servicios de telecomunicaciones.

Investigación judicial

El Pacto Internacional de Derechos Civiles y Políticos establece que "nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación". Para darle vigencia a esta garantía, añade que toda persona gozará de la protección legal contra tales interferencias.[8] En términos idénticos, la Convención Americana sobre Derechos Humanos reconoce el derecho a la intimidad.[9]

Ambos instrumentos internacionales hacen parte del bloque de constitucionalidad. Esto es, al establecer garantías sobre los derechos hu-

Creepy, Long-Standing Practice of Undersea Cable Tapping", 16 de julio de 2013. Recuperado de: http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/ (consultado el 19 de marzo de 2014).

6 Para una explicación detallada sobre la inspección profunda de paquete, ver Cortés (2014c).

7 Cfr. Corte Constitucional, sentencias T-708 de 2008, M.P. Clara Inés Vargas, y C-540 de 2012, M.P. Jorge Iván Palacio Palacio.

8 Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas, artículo 17.

9 Convención Americana sobre Derechos Humanos, artículo 11, numerales 1 a 3.

manos y haber sido incorporados válidamente al marco normativo colombiano, tienen el mismo rango que la Constitución Nacional. Esta última, en la misma línea de las definiciones anteriores, en su artículo 15 garantiza el derecho a la intimidad en los siguientes términos:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
>
> En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
>
> La correspondencia y demás formas de comunicación privadas son inviolables. Solo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

De manera complementaria, el artículo 28 de la Constitución se relaciona con el derecho a la intimidad, al establecer que toda persona es libre y que, entre otras, su domicilio solo puede ser registrado "en virtud de mandamiento escrito de autoridad judicial competente, con las formalidades legales y por motivo previamente definido en la ley".

Las comunicaciones privadas son entonces inviolables, excepto cuando, en un caso previsto en la ley, un juez autoriza previamente la interceptación de conformidad con los procedimientos que contemple la misma ley. Solo con este nivel de protección se puede evitar la arbitrariedad y el abuso de una autoridad administrativa.[10]

Con la llegada del Sistema Penal Acusatorio se introdujo una excepción. El artículo 250 de la Constitución fue modificado para que la Fiscalía General de la Nación tuviera la potestad de "adelantar registros, allanamientos, incautaciones e interceptaciones de comunicaciones. En estos eventos el juez que ejerza las funciones de control de garantías efectuará el control posterior respectivo, a más tardar dentro de las treinta y seis (36) horas siguientes".[11] Es decir, se le dio la facultad a la Fiscalía para efectuar interceptaciones sin necesidad de autorización previa, pero con control judicial posterior.[12] Más adelante, la Ley 1453 de 2011 recortó el plazo de 36 a 24 horas. Teniendo en cuenta que se trataba de un desarrollo legal más garantista, la Corte declaró exequible ese ajuste.[13]

En términos del artículo 235 del Código de Procedimiento Penal, el fiscal puede entonces ordenar "que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación". La orden tiene vigencia máxima de seis meses con posibilidad de prórroga.

Según la Corte Constitucional, la Fiscalía requiere esta potestad para recaudar rápidamente aquella información que está a punto de desaparecer o ser alterada. En esa medida, la Corte calificó la excepción: solo si existe ese riesgo es legítima la interceptación, el allanamiento, la incautación o el registro, sin orden judicial.[14]

Por su parte, la labor del juez de control de garantías es examinar que la actuación de la Fiscalía se adecue a los derechos fundamentales de los ciudadanos. Este control puede tener dos resultados: si se determina que hubo alguna vulneración en contra de los sujetos investigados, esa actuación de la Fiscalía pierde legitimidad, y las pruebas recaudadas, en la mayoría de los casos, se vuelven inválidas en el proceso penal. Por el contrario, si el juez determina que la Fiscalía no desbordó los límites, aprueba lo actuado.

En particular, la actuación de la Fiscalía debe cumplir con el requisito de proporcionalidad. En palabras de la Corte Constitucional, debe verificarse "si la medida de intervención en el ejercicio del derecho fundamental (i) es adecuada para contribuir a la obtención de un fin constitucionalmente legítimo; (ii) si es necesaria por ser la más benigna entre otras posibles para alcanzar el fin; y (iii) si el objetivo perseguido con la intervención compensa los sacrificios que esta comporta para los titulares del derecho y la sociedad".[15]

El Decreto 1704 de 2012, que reglamentó una reforma al Código Penal, define la interceptación legal de comunicaciones sin hacer distinción de "origen o tecnología". Simplemente afirma que se trata de "un mecanismo de seguridad pública que busca optimizar la labor de investigación de

10 Cfr. Corte Constitucional, sentencias C-179 de 1994, M.P. Carlos Gaviria Díaz, y T-343 de 1993, M.P. Fabio Morón Díaz.

11 Constitución Política de Colombia, artículo 250, numeral 2.

12 Ley 1453, artículo 68.

13 Cfr. Corte Constitucional, sentencia C-131 de 2009, M.P. Nilson Pinilla Pinilla.

14 Cfr. Corte Constitucional, sentencias C-336 de 2007, M.P. Jaime Córdoba Triviño, y C-334 de 2010, M.P. Juan Carlos Henao Pérez.

15 Corte Constitucional, sentencia C-591 de 2005, M.P. Clara Inés Vargas.

los delitos que adelantan las autoridades y organismos competentes, en el marco de la Constitución y la ley".[16] Y, para que la autoridad judicial pueda llevarla a cabo, los proveedores de redes y servicios de telecomunicaciones deben garantizar "en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión y acceso a la captura del tráfico de las comunicaciones que cursen por sus redes".[17] O sea, deben garantizar una infraestructura amigable para el acceso o una puerta trasera para adelantar la interceptación.

La interceptación sin orden judicial –salvo la excepción de la Fiscalía– es un delito. El artículo 269C del Código Penal establece que "el que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de 36 a 72 meses".

Labores de inteligencia

El monitoreo del espectro electromagnético hace parte de las actividades de inteligencia y contrainteligencia del Estado. Se trata de una labor inscrita en los fines del Estado de "defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo",[18] y en los objetivos de la Policía Nacional y las Fuerzas Militares de defender la soberanía nacional, la integridad del territorio nacional y el orden constitucional.[19]

El artículo 2 de Ley de Inteligencia (Ley Estatutaria No. 1621 de 2013) establece que las labores de inteligencia y contrainteligencia implican la "recolección, procesamiento, análisis y difusión de información" para prevenir y combatir amenazas de origen interno o externo contra el régimen democrático, constitucional y legal, y contra la seguridad y la defensa nacional.

La Policía y las Fuerzas Militares, a través de las dependencias especializadas para ese fin, están autorizadas para llevar a cabo actividades de inteligencia y contrainteligencia. Adicionalmente, puede hacerlo la Unidad de Información y Análisis Financiero –una entidad dedicada a combatir el lavado de activos– y cualquier otra entidad autorizada por ley. Esto implica que la Dirección Nacional de Inteligencia, creada en 2011 para reemplazar el Departamento Administrativo de Seguridad, goza también de esa facultad.[20]

Según el artículo 17 de la Ley de Inteligencia, "la interceptación de conversaciones privadas telefónicas móviles o fijas, así como de las comunicaciones privadas de datos, deberán someterse a los requisitos establecidos en el artículo 15 de la Constitución y el Código de Procedimiento Penal y sólo podrán llevarse a cabo en el marco de procedimientos judiciales". Esto es, requieren el mismo nivel de control judicial que las investigaciones generales. El monitoreo del espectro, en cambio, "no constituye interceptación de comunicaciones".

Según la Corte, el monitoreo del espectro consiste en llevar a cabo "maniobras preventivas de inspección",[21] e implica "una especie de rastreo de sombras, imágenes y sonidos representados en frecuencias de radiación electromagnética y ondas radioeléctricas".[22] En oposición a la interceptación, que implica una acción individual y dirigida, el monitoreo supone "la captación incidental de comunicaciones en las que se revelan circunstancias que permiten evitar atentados y controlar riesgos para la defensa y seguridad de la Nación".[23]

El monitoreo es –siguiendo el criterio de la Corte– una actividad pasiva que se hace bajo el supuesto razonable de que se está cometiendo o preparando un delito. Solo debe llevarse a cabo "para conseguir la información que sea estrictamente necesaria sobre operaciones sospechosas o fraudulentas, durante un lapso de tiempo minucioso, sin vulnerar el derecho a la intimidad y afianzando la reserva correspondiente para garantizar

16 Decreto 1704 de 2012, artículo 1.
17 Ibíd., artículo 2.
18 Constitución Política, artículo 2, parcial.
19 Cfr. Constitución Política, artículos 217 y 218. Ver también Corte Constitucional, sentencias C-913 de 2010, M.P. Nilson Pinilla Pinilla; T-066 de 1998, M.P. Eduardo Cifuentes Muñoz, y T-444 de 1992, M.P. Alejandro Martínez Caballero.
20 Ley de Inteligencia, artículo 3. Por otra parte, la Ley 1444 de 2011 en el literal a) del artículo 18 reviste al Presidente de la República con la facultad extraordinaria de crear departamentos administrativos. En consecuencia, a través del Decreto 4179 de 2011 se creó la Dirección Nacional de Inteligencia, que funciona como "un organismo civil de seguridad, que desarrolla actividades de inteligencia estratégica y contrainteligencia" (artículo 1). Para efectos de la Ley 1621 de 2013, la DNI es entonces un organismo que lleva a cabo funciones de inteligencia y contrainteligencia.
21 Corte Constitucional, sentencia T-708 de 2008, M.P. Clara Inés Vargas.
22 Corte Constitucional, sentencia C-540 de 2012, M.P. Jorge Iván Palacio Palacio.
23 Idem.

el buen nombre de las personas".[24] Además, debe ser proporcional, estar sujeto a procedimientos legales, ejecutarse bajo controles y supervisión, y prever mecanismos de reclamación para los afectados.[25]

La Ley de Inteligencia, sin embargo, no contempla forma alguna de reclamación para un particular afectado por labores de inteligencia, y establece mecanismos de control y supervisión en los siguientes términos:

- El monitoreo del espectro electromagnético, como cualquier actividad de inteligencia, debe estar autorizado en una orden de operaciones o una misión de trabajo, que pueden emitir los directores de los organismos o los jefes o subjefes de las unidades, secciones o dependencias particulares dentro de cada organismo, según corresponda (artículo 14).
- El nivel de autorización que requiera una orden de operaciones o misión de trabajo debe tener en cuenta "su naturaleza y posible impacto, el tipo de objetivo, el nivel de riesgo para las fuentes o agentes y la posible limitación de derechos fundamentales" (artículo 14).
- La información recolectada que no sirva para cumplir con los fines mencionados debe "ser destruida y no podrá ser almacenada en las bases de datos de inteligencia y contrainteligencia" (artículo 17).
- Las faltas a los deberes u obligaciones que cometan los funcionarios encargados de las actividades de inteligencia serán causal de mala conducta y podrán originar responsabilidad civil, penal, fiscal o profesional. La exención de responsabilidad por obediencia debida no opera en casos de violaciones a los derechos humanos o al derecho internacional humanitario (artículo 15).
- Se crea la Comisión legal de seguimiento a las actividades de inteligencia y contrainteligencia dentro del Congreso de la República. Su objetivo es controlar políticamente el uso de recursos y el respeto de la Ley de Inteligencia en estas actividades (artículo 20).
- El inspector de la Policía o de la fuerza militar de la que se trate, o quien haga sus veces (en el caso de UIAF y la Dirección Nacional de Inteligencia) debe rendir un informe anual reservado ante el Ministerio de Defensa, con copia a la Comisión legal de seguimiento de actividades de inteligencia y contrainteligencia del Congreso, sobre la observancia de los principios y límites establecidos en la Ley de Inteligencia (artículo 18).
- La parte final del artículo 18 establece que los inspectores contarán con la colaboración de los "diferentes organismos, quienes en ningún caso podrán revelar sus fuentes y métodos". No obstante, al estudiar la constitucionalidad de este artículo, la Corte manifestó que esa reserva "no es óbice para que puedan acceder únicamente los organismos de control y supervisión a efectos de poder cumplir de manera efectiva la función que les ha sido encomendada. Condición de no revelación que tampoco podrá alegarse frente a una autoridad judicial en el curso de una investigación".[26]
- Los funcionarios de estos organismos están obligados a reportar irregularidades en el ejercicio de la actividad de inteligencia al inspector correspondiente o al director o jefe del organismo de inteligencia. Los directores o jefes, a su vez, deben rendir informe anual al Presidente sobre estas irregularidades (artículo 18).

Datos sobre usuarios

Como vimos, los datos de los usuarios en poder de los operadores de servicios de telecomunicaciones son fundamentales para la vigilancia moderna. No solo son un complemento o el punto de arranque de una investigación; por sí solos pueden llegar a ser suficientes para monitorear las actividades de una persona. Aquí nuevamente es necesario hacer una distinción entre las labores de investigación judicial y aquellas circunscritas a la inteligencia y contrainteligencia estatal.

El Decreto 1704 de 2012 establece, a título ilustrativo y no taxativo, el tipo de información del suscriptor que los proveedores de redes y servicios de telecomunicaciones deben entregar.[27] Según el artículo 4, los operadores deben suministrar a la Fiscalía General de la Nación o "demás autoridades competentes", los datos del suscriptor, "tales como identidad,

24 Cfr. Corte Constitucional, sentencia T-708 de 2008, M.P. Clara Inés Vargas.

25 Cfr. Corte Constitucional, sentencia C-540 de 2012, M.P. Jorge Iván Palacio Palacio. Ver también, Corte Constitucional, sentencia T-1037 de 2008, M.P. Jaime Córdoba Triviño.

26 Corte Constitucional, sentencia C-540 de 2012, M.P. Jorge Iván Palacio Palacio.

27 El decreto opta por este nombre en vez del de "operadores de servicios de telecomunicaciones" que usa la Ley de Inteligencia.

dirección de facturación y tipo de conexión. Esta información debe entregarse de forma inmediata".[28]

Podría decirse que este artículo se refiere únicamente a los datos que permiten identificar al suscriptor. En ese caso, información como el historial de navegación o el listado de llamadas realizadas, no podría solicitarse con fundamento en esta norma. Sin embargo, al referirse a datos "tales como", el Decreto parece ambiguo.

Adicionalmente, el artículo 5 obliga a los proveedores a entregar, para efectos de interceptación de comunicaciones, "la información específica contenida en sus bases de datos, tal como sectores, coordenadas geográficas y potencia, entre otras, que contribuya a determinar la ubicación geográfica de los equipos terminales o dispositivos que intervienen en la comunicación. Esta información deberá suministrarse en línea o en tiempo real en los casos que así se requiera".

En 2007, la Corte Constitucional dispuso que la búsqueda selectiva en bases de datos de entidades públicas o privadas requiere orden judicial.[29] Este requisito, sin embargo, no existe en materia de inteligencia y contrainteligencia. Según el artículo 44 de la Ley de Inteligencia, los operadores de servicios de telecomunicaciones tienen una obligación de colaboración. Esto implica, en concreto, que por solicitud de una agencia de inteligencia del Estado, y en desarrollo de una operación autorizada, el operador debe suministrar "el historial de comunicaciones de los abonados telefónicos vinculados, los datos técnicos de identificación de los suscriptores sobre los que recae la operación, así como la localización de las celdas en que se encuentran las terminales y cualquier otra información que contribuya a su localización".

Los operadores están obligados a almacenar la información de los usuarios por un periodo de cinco años.[30] Nuevamente, no queda claro si esta obligación abarca también los datos de los usuarios relacionados con los servicios. De ser así, este término excede largamente los estándares internacionales. Solo para ilustrar este punto, recientemente la Corte Europea de Justicia declaró inválida la directiva europea sobre retención de datos. Para la Corte, el periodo de retención de datos de la directiva –de 6 a 24 meses– no podía plantearse de manera genérica, sino que debía adaptarse a partir de objetivos específicos.[31]

28 En julio de 2013, el Consejo de Estado suspendió provisionalmente la frase "demás autoridades competentes", mientras resuelve un recurso de nulidad contra el decreto.

29 Cfr. Corte Constitucional, sentencia C-336 de 2007, M.P. Jaime Córdoba Triviño.

30 Ley de Inteligencia, artículo 44, y Decreto 1704 de 2012, artículo 4.

31 Corte Europea de Justicia, Digital Rights Ireland Ltd (C-293/12) *vs.* Minister for Communications, Marine et ál., 8 de abril de 2014. Recuperado de: http://malte-spitz.de/wp-content/uploads/2014/04/C_0293_2012-EN-ARR.pdf (consultado el 20 de mayo de 2014).
Cfr. Corte Europea de Derechos Humanos. Halford *vs.* Reino Unido, 1997.

Interceptación de comunicaciones en otros países

Tres puntos fundamentales saltan a la vista después de revisar el marco normativo colombiano sobre vigilancia de comunicaciones en desarrollo de actividades de inteligencia: la distinción entre monitoreo e interceptación, los requerimientos diferenciados para llevarlas a cabo y el tipo de control sobre unas y otras.

Al ser este punto el eje principal del documento, a continuación hacemos una breve referencia comparada. Como veremos, en los países estudiados, el monitoreo y la interceptación hacen parte por igual de las actividades de inteligencia y, en consecuencia, están sujetos a los mismos controles. Estos últimos, además, suelen inscribirse en instancias de control internas o con un tipo de supervisión judicial especial.

Reino Unido

La interceptación de comunicaciones en el Reino Unido está regulada por la Ley RIPA de 2000 (*Regulation of Investigatory Powers Act*). Resulta útil situarla brevemente en contexto: en 1984, en el caso Malone contra el Reino Unido, la Corte afirmó que Inglaterra y Gales violaban la Convención Europea de Derechos Humanos al no tener ningún tipo de regulación sobre interceptación telefónica, lo cual desembocaba en el desconocimiento del artículo 8 de la Convención, sobre privacidad y vida familiar (Oxford Pro Bono Publico 2006).

Fruto de esta decisión, el Parlamento expidió en 1985 el Acto de Interceptación de Comunicaciones. Esta vez, la Corte Europea lo consideró insuficiente al centrarse en comunicaciones enviadas por correo postal o por un sistema de telecomunicación pública, en detrimento de las comunicaciones privadas, que quedaban exentas de los controles legales.[32] Este antecedente, sumado a la promulgación del Acto de Derechos Humanos

de 1998 –que incorporaba toda la carta de derechos de la Convención–, dieron origen a RIPA, que propone un marco legal más amplio frente a los poderes de vigilancia del Estado.

RIPA regula entonces actividades de vigilancia encubierta del Estado, como el uso de rastreadores, cámaras ocultas e interceptación de comunicaciones –desde llamadas hasta correos electrónicos–. Cobija, entre otros, a la Policía, los servicios de inteligencia (MI5, MI6 y GCHQ) e incluso agencias de los gobiernos locales (Open Rights Group 2013). La interceptación de comunicaciones se define como cualquier acción encubierta para adquirir los contenidos de mensajes o conversaciones que transitan por una red o son distribuidos por un servicio (Justice 2011).

La Sección Primera de RIPA establece que es una ofensa criminal interceptar intencionalmente las comunicaciones de cualquier persona sin contar con la "autoridad legal" (*lawful authority*). "Autoridad legal" es una orden emitida por el Secretario de Estado o el Secretario de Interior (en el caso de Inglaterra, son la mayoría de los ministros que están a cargo de un departamento del Gobierno). Corresponde al Secretario corroborar que la interceptación se hace en interés de la seguridad nacional, con el propósito de prevenir o detectar un crimen grave o con el de salvaguardar el interés económico del Reino Unido.[33]

No obstante, en las siguientes circunstancias no se requiere dicha orden para llevar a cabo la interceptación:

- Las dos partes consienten la interceptación o se cree razonablemente que han dado su consentimiento.
- Una de las partes ha dado el consentimiento –por ejemplo, cuando una de las partes es la que graba la conversación– y la vigilancia es dirigida (una categoría de RIPA que se refiere a un tipo de vigilancia que, aunque es encubierta, no implica entrar a un domicilio o espacio privado y se hace en desarrollo de una operación o investigación).
- La comunicación tiene lugar en una red privada de telecomunicaciones (una empresa, por ejemplo) y la interceptación cuenta con el consentimiento de quien controla el sistema (en otras palabras, el jefe).
- La comunicación se hace desde o hacia una cárcel o un hospital psiquiátrico.
- Para que la petición de una interceptación de comunicaciones pueda ser aprobada, el secretario de estado tiene que asegurarse de que sea necesaria para a) el interés de la seguridad nacional, 2) prevenir o detectar el crimen y 3) salvaguardar el bienestar económico del Reino Unido.

La supervisión de las órdenes de interceptación está a cargo del Comisionado para la Interceptación de Comunicaciones, que debe ocupar o haber ocupado una posición alta en la Rama Judicial.[34] El Comisionado tiene la responsabilidad de mantener bajo revisión las órdenes de interceptación, pero no tiene competencia para revisar el proceso o la justificación que subyace a cada orden.

La instancia que sí tiene esa potestad es el Tribunal de Poderes Investigativos, que tramita las quejas contra cualquier entidad pública en relación con interceptaciones de comunicaciones y otras actividades autorizadas bajo RIPA. Concretamente, el Tribunal puede anular órdenes de interceptación o disponer de la destrucción de cualquier materia fruto de la vigilancia.[35] No obstante, las decisiones de RIPA no pueden ser apeladas ni cuestionadas ante ninguna corte. Tampoco hay audiencias orales, alegatos, interrogatorios o instancias para cuestionar pruebas. En últimas, una persona que tenga razones para creer que ha sido objeto de interceptaciones irregulares, no puede tener ninguna expectativa de que el tribunal resuelva su caso o le entregue información sobre el particular (Justice 2011).

Chile

La ley chilena sobre el Sistema de Inteligencia del Estado reconoce que cuando exista necesidad de obtener cierta información no disponible por medio de "fuentes abiertas", se podrán emplear "procedimientos especiales de obtención de información" para resguardar la seguridad nacional y proteger "a Chile y a su pueblo de las amenazas del terrorismo, el crimen organizado y el narcotráfico".[36]

Los procedimientos autorizados para acceder a "fuentes cerradas" son los siguientes:

a) La intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas.

33 RIPA, sección 5 (5).

34 RIPA, sección 57 (5).

35 RIPA, sección 67 (7)

36 Ley 19.974 de 2004, artículo 23.

b) La intervención de sistemas y redes informáticos.
c) La escucha y grabación electrónica, incluyendo la audiovisual.
d) La intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información.[37]

El uso de cualquiera de estos procedimientos requiere autorización judicial. El director o jefe de los organismos de inteligencia debe solicitarla, y solo se le otorgará para detectar, neutralizar o contrarrestar las acciones de grupos terroristas, nacionales o internacionales, y de organizaciones criminales transnacionales, o las acciones de inteligencia de otros grupos nacionales o extranjeros.[38]

La ley chilena también dispone que la resolución que autorice los procedimientos "deberá incluir la especificación de los medios que se emplearán, la individualización de la o las personas a quienes se aplicará la medida y el plazo por el cual se decreta, que no podrá ser superior a noventa días, prorrogable por una sola vez hasta por igual período".[39]

Las actividades de inteligencia están sujetas a controles internos y externos. El primero es competencia del director o jefe de cada organismo de inteligencia, que además es el responsable directo del cumplimiento de la ley. Este control comprende el uso de recursos humanos y técnicos, del empleo racional de los fondos que le han asignado y del respeto a las garantías constitucionales y legales en desarrollo de sus operaciones.[40]

El control externo, por su parte, será ejercido por la Contraloría General de la República y la Cámara de Diputados. A la primera le corresponde hacer un control de legalidad reservado –conocido como "toma de razón"– de los actos de la Agencia Nacional de Inteligencia.[41] A la Cámara de Diputados le corresponde, a través de una Comisión Especial, conocer los informes de actividades de los organismos de inteligencia en sesiones reservadas.[42]

La norma incluye también a los tribunales de justicia como entidades de control externo, pero no especifica sus potestades más allá de indicar que deben hacerlo dentro de "sus respectivas competencias".[43] De cualquier forma, el deber de reserva de las actividades de inteligencia no puede oponerse a las solicitudes que hagan los tribunales de justicia, la Cámara de Diputados y el Ministerio Público, entre otros.[44]

México

El artículo 16 de la Constitución Política de México dispone que únicamente la autoridad judicial federal, a petición de la autoridad federal competente o del Ministerio Público del estado correspondiente, puede autorizar la interceptación de una comunicación privada. La autoridad interesada debe incluir en la solicitud la justificación de la actividad, la duración, el tipo de intervención, los sujetos implicados y la duración.

Por su parte, la Ley de Seguridad Nacional mexicana somete las intervenciones de comunicaciones con fines de inteligencia y contrainteligencia a un estándar especial de control judicial. En términos del artículo 34, "se entiende por intervención de comunicaciones la toma, escucha, monitoreo, grabación o registro, que hace una instancia autorizada, de comunicaciones privadas de cualquier tipo y por cualquier medio, aparato o tecnología".[45] La intervención, entonces, abarca por igual las actividades de interceptación y monitoreo.

La intervención de comunicaciones en los términos de la Ley de Seguridad solo procede cuando existan amenazas a la seguridad nacional, que implican, entre otras, espionaje, sabotaje, terrorismo, rebelión y traición a la patria (artículo 5). En esos casos, las autoridades tendrán que seguir un procedimiento reservado para obtener la autorización, la cual debe resolverse dentro de las 24 horas siguientes a la solicitud. Esta última debe incluir una descripción de los hechos –omitiendo los detalles que pongan en riesgo la operación–, la justificación y el tiempo por el que se pide la intervención.

En la resolución que admite la medida, el juez debe incluir el tipo de actividad que se llevará a cabo, el lapso para ejecutarla y la autorización para instalar o remover equipos relacionados con la operación (artículo 37 y ss.). La autorización se otorga por máximo 180 días con posibilidad de prórroga por el mismo periodo. Eventualmente, el juez puede solicitar

37 Ibíd., artículo 24.
38 Ibíd., artículos 25 y 27.
39 Ibíd., artículo 28.
40 Ibíd., artículos 33 y 34.
41 Ibíd., artículo 36.
42 Ibíd., artículo 37.
43 Ibíd., artículo 36.
44 Ibíd., artículo 39.
45 Congreso de los Estados Unidos Mexicanos, Ley de Seguridad Nacional. Diario Oficial de la Federación de 31 de enero de 2005. Recuperado de: http://mexico.justia.com/federales/leyes/ley-de-seguridad-nacional/ (consultado el 3 de abril de 2014).

informes periódicos sobre la ejecución de la autorización que, de ninguna forma, puede divulgar –él o cualquiera de los funcionarios de ese despacho (artículo 45 y ss.).

Las acciones relacionadas con seguridad nacional están sujetas al control legislativo. Para el efecto, la ley crea un comisión bicameral, compuesta por tres senadores y tres diputados, que tiene la atribución de pedir informes específicos al Centro de Investigación y Seguridad Nacional, conocer los demás reportes generales y hacer recomendaciones sobre cualquier tema. En cualquier caso, el Centro puede abstenerse de revelar información que ponga en riesgo la seguridad nacional, y la Comisión, a su vez, está obliga a mantener la reserva (artículo 57 y ss.).

En busca de un sistema balanceado

A la luz de la tecnología moderna, el régimen colombiano en materia de vigilancia de comunicaciones presenta, al menos, tres problemas: i) aunque existe una distinción conceptual entre el monitoreo del espectro radioeléctrico y la interceptación de comunicaciones, en la práctica se superponen: de una actividad de monitoreo puede derivarse una interceptación, o en desarrollo de una interceptación puede monitorearse el espectro; ii) sin tener una definición granular, la interceptación de comunicaciones puede desembocar en esquemas de vigilancia masiva o desproporcionada contra el individuo; iii) en combinación con las demás herramientas de vigilancia, el acceso a los datos de los usuarios constituye un riesgo adicional de vulneración de derechos fundamentales.

Estos puntos convergen de una u otra forma en las definiciones y los controles. Por un lado, es necesario que la regulación y la jurisprudencia interpreten adecuadamente la capacidad y el funcionamiento de los esquemas de vigilancia moderna. Pero cualquier avance al respecto será inútil si los controles cotidianos a la vigilancia desconocen de plano las garantías constitucionales mínimas y los derechos humanos.

A continuación se referencian los derechos en juego, haciendo énfasis en la privacidad. Posteriormente, retomaremos la discusión planteada y, finalmente, haremos consideraciones a manera de conclusión.

La privacidad y otros derechos en juego

Más allá de si se hace en el contexto de un proceso judicial o en desarrollo de actividades de inteligencia del Estado, la vigilancia y el monitoreo de las comunicaciones entran en tensión con el derecho fundamental a la intimidad. Tanto así que el artículo 15 de la Constitución plantea la interceptación y el registro de las comunicaciones como una excepción a la intimidad familiar y la privacidad de las comunicaciones. No es, sin embargo, el único derecho en juego. El habeas data y la libertad de expresión, la libertad de asociación y la libertad religiosa, entre otros, resultan igualmente comprometidos.

La Corte Constitucional colombiana ha usado distintas aproximaciones teóricas para definir el núcleo esencial de la privacidad o derecho a la intimidad. A lo largo de más de 20 años de jurisprudencia, el tribunal lo ha delimitado en términos espaciales, visuales e informativos –lo cual sugiere, además, la influencia de varias tradiciones jurídicas.

"El contenido básico del derecho fundamental a la intimidad presupone la existencia y goce de un espacio reservado de cada individuo que se encuentra exento de la intervención o intromisiones arbitrarias del Estado y la sociedad", dijo la Corte recientemente.[46] A este criterio espacial –en el sentido metafórico– se suma el postulado del "derecho a ser dejado solo", tomado de la doctrina norteamericana *(the right to be let alone)*:

> […] la protección constitucional del derecho a ser dejado solo, como manifestación esencial del derecho a la intimidad, tiene su soporte no solo en el hecho coyuntural de la soledad, que analizada aisladamente en nada enriquece el contenido de dicho derecho, sino en la seguridad de no ser observado, y de poder actuar sin el miedo de que alguien, en cualquier momento, revelará una acción o esfera exclusiva de su comportamiento.[47]

La Corte resume entonces la vulneración del derecho a la intimidad en tres escenarios: i) "la intromisión irracional en la órbita que cada persona se ha reservado"; ii) la divulgación de hechos privados, y iii) la divulgación tergiversada o falsa de asuntos personales, que –según el tribunal– se relacionan ya con el derecho a la honra y el buen nombre.[48]

Más allá de la jurisprudencia citada, las metáforas visuales están menos presentes en la jurisprudencia constitucional. La idea de que el derecho a la intimidad no se limita a un espacio (la casa, el trabajo, el cuerpo), sino también al interés del individuo de no ser observado en ciertas circunstancias, permite extender el alcance de este derecho. La posibilidad de observar a la persona va más allá de su presencia física e incluye cual-

46 Corte Constitucional, sentencia C-540 de 2012, M.P. Jorge Iván Palacio.
47 Corte Constitucional, sentencia C-787 de 2004, M.P. Rodrigo Escobar Gil.
48 Ibíd.

quier contenido –una información, un dato, una fotografía– que la represente o que diga cualquier cosa sobre ella, más allá de donde se encuentre.

Por otra parte, la observación como vulneración a la privacidad no se define únicamente en términos de la acción de observar. Es decir, el monitoreo generalizado y la interceptación desproporcionada de las comunicaciones no resultan problemáticos solo por el hecho de que una persona acceda a información sobre el individuo y, eventualmente, la almacene o la divulgue. La vigilancia generalizada, en sí misma, modifica el entorno de la persona, la vuelve consciente de su propia subjetividad y la priva del confinamiento voluntario necesario para desarrollar su individualidad.

Benn considera que la observación extendida inhibe la disposición para escoger. La observación, afirma, "lo sitúa a uno en un plano nuevo de conciencia sobre uno mismo, como algo visto a través de los ojos de otra persona". Julie Cohen coincide, y afirma que la observación generalizada constriñe la espontaneidad y lleva al individuo hacia lo insípido (Kang 1998: 1260, Cohen 2000: 1373).

Constreñir la espontaneidad y crear previsibilidad es de hecho el propósito de políticas de vigilancia pública como las cámaras de circuito cerrado. Bajo el lente que observa, la gente se comporta de maneras preestablecidas (Cohen 2012: 575). Trasladar estos esquemas –de por sí cuestionables– a todas las órbitas del individuo, estrechan la privacidad y afectan el libre desarrollo de la personalidad.

Es acá donde queda claro que el derecho a la libertad de expresión está también en juego cuando la órbita privada del individuo desaparece. Por un lado, la ausencia de un espacio de reclusión impide la reflexión, la experimentación, el desarrollo de convicciones e interpretaciones sobre la realidad. Por el otro, la inminencia de la observación externa obliga al individuo a pasar sus opiniones por el filtro de esa mediación –oficial o privada–. Parafraseando al escritor George Mangakis, quien se refería a la práctica de las autoridades penitenciarias de revisar la correspondencia de los reclusos, el riesgo es que el individuo termine controlando sus propios pensamientos a la luz de quien observa (Mangakis 2007: 56). En pocas palabras, sin privacidad, la libertad de expresión es solo una apariencia.

La negación de la privacidad también imposibilita el ejercicio de otras garantías constitucionales, como la reserva de la fuente para los periodistas, que se inscribe en el derecho general al secreto profesional.[49] Para la Corte Constitucional, "la conexión evidente entre el secreto profesional y otros derechos fundamentales fortalece, aún más, el derecho a la intimidad y el mandato de inviolabilidad de las comunicaciones privadas".[50]

Por último, la privacidad tiene una relación estrecha con el derecho al habeas data, que –como vimos– hace parte también del artículo 15 de la Constitución, el cual reconoce que todas las personas "tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas", y agrega que "en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".

Definiciones y controles

Durante el proceso de revisión de la Ley de Inteligencia ante la Corte Constitucional, algunas organizaciones de la sociedad civil hicieron la advertencia que en gran parte motivó este documento: el monitoreo del espectro radioeléctrico requiere las mismas garantías constitucionales que la interceptación de comunicaciones.

En su intervención ante la Corte, la Defensoría del Pueblo consideró que la afirmación "el monitoreo no constituye interceptación de comunicaciones" va en contra de la Constitución.[51] Cualquier tipo de "vigilancia" o "supervisión" del espectro –afirmó la entidad– recaería eventualmente sobre comunicaciones personales y, por lo tanto, desembocaría en vulneraciones de los derechos fundamentales.

En ese mismo sentido, Dejusticia y la Fundación para la Libertad de Prensa (FLIP) argumentaron que el monitoreo es una forma de interceptación: "El barrido al espectro electromagnético es una intervención directa sobre la intimidad de las personas".[52] Para estas organizaciones, la ausencia de una orden judicial deja inerme al ciudadano frente a la privacidad y seguridad de sus comunicaciones personales.

Para la Corte, como se vio anteriormente, el monitoreo del espectro no puede constituir un seguimiento individual porque no implica un "rastreo selectivo" de un sujeto individualizado. Adicionalmente, en un argumento que no se compadece con la importancia del caso y el nivel de

49 Cfr. Corte Constitucional, sentencia T-298 de 2009, M.P. Luis Ernesto Vargas.

50 Corte Constitucional, sentencia T-708 de 2008, M.P. Clara Inés Vargas.

51 Corte Constitucional, sentencia C-540 de 2012, M.P. Jorge Iván Palacio Palacio.

52 Idem.

quienes lo abordaron, la Corte planteó que el monitoreo no podía constituir una interceptación de comunicaciones privadas porque para esto se requiere orden judicial.

Por supuesto, este razonamiento no resuelve el dilema práctico. El hecho de que la interceptación de comunicaciones requiera orden judicial no desdice de la naturaleza de la actividad. Al contrario, si prosperara la afirmación de que ambas prácticas son similares y comprometen el ejercicio de derechos fundamentales, la conclusión debería apuntar a que deben estar sometidas al mismo estándar legal.

En enero pasado, las personas que participaban en las protestas ciudadanas en Kiev (Ucrania) recibieron el siguiente mensaje de texto en sus celulares: "Estimado suscriptor, usted está registrado como participante de unos disturbios masivos".[53] Las empresas de telefonía móvil negaron cualquier responsabilidad en el hecho, lo cual es posible. El gobierno del entonces presidente Viktor Yanukovych bien pudo haber pedido los registros de todos los teléfonos móviles conectados a determinadas estaciones base –un procedimiento conocido como *tower dumps*–, o usado un *Stingray* para suplantar una de estas bases y obtener directamente la información de los usuarios en la zona.[54] Es decir, usó una tecnología para "monitorear" el espectro. Al cruzarlo con la identidad de los suscriptores, pudo armar fácilmente un censo de quienes protestaban. No hay razón para descartar que algo así se pueda hacer en Colombia.

Ninguno de los tres países observados hace en su legislación la distinción del régimen colombiano. Aunque en el Reino Unido y en Chile no se hace una mención explícita del monitoreo, este parece quedar comprendido dentro de las actividades de vigilancia. En México, en cambio, el artículo 34 de Ley de Seguridad Nacional sí incluye explícitamente el monitoreo dentro de lo que se denomina "intervención de comunicaciones" –que también incluye la interceptación.

Que el monitoreo del espectro radioeléctrico estuviera sujeto a las mismas reglas de la interceptación implicaría –en nuestro caso– que tendría control judicial. No obstante, ahí las salvaguardas también parecen insuficientes. Si bien el artículo 235 del Código Penal se refiere a la potestad del fiscal de interceptar comunicaciones "que cursen por cualquier red de comunicaciones", y el Decreto 1704 de 2012 habla de cualquier "origen o tecnología", ninguna norma –y mucho menos la jurisprudencia– desarrolla criterios frente a los medios empleados.

¿Es legal interceptar las comunicaciones de una persona mediante métodos engañosos y potencialmente desproporcionados como los *troyanos*? ¿Qué sucede cuando al emplear estos mecanismos se afecta la propiedad del sujeto, por ejemplo, al dañar su computador? ¿Qué garantía tienen los usuarios de un equipo o de una red que está siendo objeto de análisis de tráfico –con tecnologías como la *inspección profunda de paquete*– con el propósito de interceptar las comunicaciones de un solo individuo? ¿Qué garantías existen para que una vez la interceptación legal finalice, los dispositivos de vigilancia sean desactivados?

A diferencia de las interceptaciones telefónicas tradicionales, e incluso de las que se hacen sobre teléfonos móviles, la vigilancia en Internet es menos costosa. Mientras que en los demás casos las autoridades deben invertir recursos y frecuentemente contar con la colaboración del operador, un computador infectado no implica un costo para quien vigila –salvo por el costo del software maligno–. No existen incentivos para detener la actividad. Más bien, su grado de invisibilidad y latencia invitan a mantener abierto el canal. Sin controles adecuados, la interceptación en estos términos tiene un comienzo, pero no parece tener un final.

De ahí que sea tan importante que las prácticas que se autorizan estén específicamente prescritas. No es lo mismo autorizar una interceptación de un teléfono por un mes que autorizar la instalación subrepticia de un *troyano* por el mismo periodo. Y esa diferencia debe quedar clara para quien autoriza la operación. Sobre el particular, la ley mexicana, con buen criterio, establece que al emitir la autorización, el juez debe precisar, entre otros, "el tipo de actividad que autoriza" y, cuando sea necesario, "la autorización expresa para instalar o remover cualquier instrumento o medio de intervención".[55]

Es cierto que la Corte Constitucional –como se vio antes– establece que la autoridad judicial debe verificar que la medida sea adecuada para

53 Cfr. *The Guardian*. 2014. "Text messages warn Ukraine protesters they are 'participants in mass riot'", 21 de enero. Recuperado de: http://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot (consultado el 20 de marzo de 2014).

54 Cfr. *Here and Now*. 2014. "A Lesson from Ukraine on Cell Phone Metadata", 24 de enero. Recuperado de: http://hereandnow.wbur.org/2014/01/24/ukraine-metadata-lesson (consultado el 20 de marzo de 2014).

55 *Op. cit*., Congreso de los Estados Unidos Mexicanos. Ley de Seguridad Nacional de México, artículo 37.

alcanzar el fin, que sea la más benigna entre otras posibles y que resulte beneficiosa frente al sacrificio que implica.[56] Sin embargo, se trata de criterios de proporcionalidad generales que se plantean en un contexto, tanto en la regulación como en la jurisprudencia, donde se omite cualquier mención a la tecnología y su impacto en el ejercicio de derechos fundamentales. Dicho de otra forma, no hay ninguna hoja de ruta para interpretar esos criterios desde esa perspectiva.

La imprecisión y vaguedad del precedente constitucional en este aspecto es reiterado. En 2008, por ejemplo, afirmó la Corte:

> En conclusión, el ejercicio de las labores de control y vigilancia sobre el espectro electromagnético así como el uso que de las frecuencias designadas para socorro y seguridad nacional hagan los organismos de inteligencia autorizados para ello, encuentran como límite los derechos fundamentales los cuales no pueden ser vulnerados so pretexto del adelantamiento de tales actividades. En efecto, las autoridades de policía conservan la facultad de monitoreo del espectro electromagnético siempre y cuando no vulneren el derecho a la intimidad de las personas.[57]

Y si bien México, Chile y el Reino Unido pueden tener mejores criterios que Colombia para la aplicación de los controles, se inscriben en sistemas que no gozan de muchas garantías. En el Reino Unido, el Comisionado para la Interceptación de Comunicaciones no tiene poderes concretos, y el Tribunal de Poderes Investigativos es una instancia secreta (Justice 2011); en México, el control es netamente político y está en manos de una comisión bicameral, similar a Chile, donde, sin embargo, hay posibilidades de control externo a cargo de la Contraloría y los tribunales de justicia.

En Colombia, en contraste, la interceptación con fines de inteligencia está sujeta a los mismos controles que la que se adelanta en desarrollo de un proceso judicial. No ocurre lo mismo, repetimos, con el monitoreo y el acceso a datos de los usuarios, cuya supervisión y control es interna y eventualmente política, en medio de una reserva absoluta.

En la sentencia que revisó la Ley de Inteligencia, el magistrado Luis Ernesto Vargas hizo un salvamento de voto y, sobre el particular, manifestó que el informe anual de los encargados de las agencias de inteligencia dirigido al Presidente debería ser público, salvo lo que realmente tuviera que estar en reserva. De lo contrario, dijo, "conlleva un nivel de abstracción, generalidad y ambigüedad que raya con la afectación del principio de legalidad al tratarse de una restricción de un derecho fundamental, como lo es de la información y transparencia de todas las actuaciones de las autoridades administrativas".

Además del monitoreo, el acceso a los datos de los usuarios representa una herramienta poderosa en términos de vigilancia y rastreo. La legislación vigente en materia de inteligencia posibilita la entrega, sin orden judicial, de todo tipo de información en manos de operadores de servicios y de redes. Pero aún no es claro si se trata únicamente de metadatos o también de datos, de contenidos de comunicaciones (un chat o un mensaje en una red social, por ejemplo), en cuyo caso equivale a una interceptación.

Como se expuso al comienzo de este documento, la información de localización del usuario se va almacenando en los registros históricos del operador del servicio. Al sumar y procesar todos estos datos, se obtiene una radiografía fiel de lo que hizo una persona en un periodo determinado. Dónde estuvo, cuándo, a qué hora, por cuánto tiempo. Para ilustrar este punto, en 2011, el político alemán del Partido Verde Malte Spitz pidió a su operador móvil que le entregara sus registros de localización de los últimos seis meses. Con esta información, el diario *Zeit* elaboró un mapa detallado de todos los movimientos de Spitz.[58] En palabras del experto en tecnología Jacob Appelbaum, al final de cuentas, "los teléfonos celulares son dispositivos de rastreo que sirven para hacer llamadas" (Crocker 2013: 622).

En su momento, la Defensoría del Pueblo le pidió a la Corte Constitucional que declarara inexequible el artículo 44 de la Ley de Inteligencia, precisamente, por no incluir alguna forma de control de las actividades previstas. En términos similares, Dejusticia y la FLIP afirmaron que acceder a estos datos sin mediación judicial alguna constituía una vulneración del derecho a la intimidad y el derecho de habeas data. Siguiendo esa línea, estas organizaciones propusieron que la Corte declarara el artículo condicionalmente ajustado a la Constitución, bajo el supuesto de que cualquier solicitud de información debía incluir una orden judicial.

56 Cfr. Corte Constitucional, sentencia C-591 de 2005, M.P. Clara Inés Vargas.

57 Corte Constitucional, sentencia T-708 de 2008, M.P. Clara Inés Vargas.

58 *Zeit Online,* "Betrayed by our own data", 26 de marzo de 2011. Recuperado de: http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz (consultado el 19 de marzo de 2014).

La Corte, sin embargo, declaró el artículo ajustado a la Carta Política. Usando un tono de condicionamiento, pero en realidad situando la norma en el contexto de los principios generales sobre inteligencia, afirmó que la solicitud del historial de comunicaciones, la identificación de los usuarios y la localización de las celdas debían sustentarse en criterios de razonabilidad y proporcionalidad, "de forma tal que el empleo de este mecanismo de colaboración se restrinja a aquellos casos en que el acopio de la información resulta imprescindible para el cumplimiento de los fines de la función de inteligencia y contrainteligencia".[59]

Aunque la Ley 1581 de 2012 desarrolla el derecho al habeas data en detalle, excluye del régimen de protección de datos personales "las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo", y "las bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia".[60]

Esto abre un espacio grande para armar expedientes sobre cualquier ciudadano sin que exista manera de controvertirlos. Ya en otra oportunidad, la Corte Constitucional se refirió al riesgo de que en los archivos de inteligencia del Estado haya información parcial, descontextualizada y sin contrastar.[61] A esto se suma el término de la retención de datos para los operadores de servicios, que en Colombia está, al parecer en cinco años, mientras en otras partes –como la Unión Europea– se limita a dos.[62] Para nuestro caso, el exceso de datos en poder de un particular o del Estado no representa solo un riesgo para la intimidad y el habeas data, sino que puede poner en riesgo la vida de una persona. Al desbordar el objetivo de este documento –y tratándose de un tema extenso y especializado– apenas dejamos delineado el problema.

Vigilancia masiva es vigilancia desproporcionada

Ni el legislador ni el juez en Colombia se están preguntando qué tipo de impacto tiene la tecnología en el ejercicio de derechos fundamentales. Al abordar preguntas relacionadas con las comunicaciones, poco o nada les interesa entender las capacidades de un esquema de vigilancia para ponderar su impacto individual. En esa medida, cualquier test de proporcionalidad estará incompleto.

Aunque sorprende que esta ausencia se dé en un país con tantos antecedentes de interceptaciones ilegales, sí es común que las tecnologías nuevas pasen por la lupa de una Corte tiempo después de su incorporación social. La situación resulta más complicada con "tecnologías inestables". A diferencia de los carros y las armas de fuego, los sistemas de comunicaciones están en un flujo constante.

En Estados Unidos, por ejemplo, las implicaciones de las interceptaciones telefónicas fueron revisadas judicialmente casi seis décadas después de que se inventara el teléfono. Hoy se requieren decisiones judiciales en temas como la inspección profunda de paquete, pero es posible que para cuando llegue una sentencia, el problema sea otro (Hosein y Wilson 2013: 1071-1104).

Kerr considera que dejarles a los jueces la labor de interpretar la tecnología es un error: "Las decisiones judiciales tienden a incorporar presunciones desactualizadas sobre la práctica tecnológica, dando lugar a reglas que tienen poco sentido en el presente o en el futuro" (Kerr 2004: 107). Los jueces –agrega– no cuentan con la información adecuada para situar los casos en el entorno más amplio de los cambios tecnológicos.

Kerr propone entonces que sea el legislador quien asuma el rol de regular tecnologías que están en flujo constante, toda vez que puede intervenir en cualquier momento, en respuesta a una preocupación pública o incluso antes de que haya un impacto negativo. El Congreso, además, no se encuentra limitado por el precedente judicial y el formalismo de la adjudicación; bien podría crear unas reglas, revisarlas y experimentar con incentivos distintos para actores privados y públicos (Kerr 2004: 163).

Sería apresurado afirmar que esa propuesta es igualmente viable en el contexto colombiano. De una parte, la Ley de Inteligencia fue una oportunidad perdida para hacer precisamente esto. De otra parte, con herramientas como la tutela, la Corte Constitucional ha impulsado el desarrollo de políticas públicas a través de casos individuales. En esa medida, bien podría asumir el rol de actualizar la interpretación de la tecnología, con la ventaja de que se trata de casos que, a diferencia de Estados Unidos, tardan menos tiempos en llegar a la última instancia. De cualquier forma, pareciera que solo una reforma legal permitiría impulsar un cambio de

59 Op. Cit. Corte Constitucional, sentencia C-540 de 2012, M.P. Jorge Iván Palacio Palacio.

60 Ley 1581 de 2012, artículo 2, literales b y c.

61 Cfr. Corte Constitucional, sentencia T-1037 de 2008.

62 Cfr. Directiva 2006/24/EC del Parlamento y el Consejo Europeo. Recuperado de: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (consultado el 4 de abril de 2014).

paradigma que, hasta ahora, no encuentra espacio en el tribunal constitucional.

Otra forma de abordar las tecnologías de vigilancia y su impacto en derechos fundamentales podría ser echando mano del principio de precaución. Este principio se aplica principalmente en el contexto de la toma de decisiones y de regulación en el campo medioambiental, aunque tiene también una acepción concreta en el campo del derecho internacional humanitario.[63] Formulado de manera sencilla, el principio de precaución postula que cuando una actividad suscite amenazas contra la salud humana o el ambiente, se deben adoptar medidas de precaución, incluso si algunas relaciones causales no están completamente establecidas científicamente.

Para la Corte, la protección del medio ambiente puede ser problemática cuando la sospecha de un daño potencial proviene de innovaciones tecnológicas o científicas que son consideradas valiosas "por contribuir a la satisfacción de necesidades humanas concretas, fomentar el comercio, la iniciativa y la inventiva privadas, o por enmarcarse en el ejercicio de profesiones liberales".[64]

Este criterio podría hacerse extensivo a la tensión entre privacidad y seguridad nacional: aplicada de manera indiscriminada o desproporcionada, una tecnología en particular podría generar un daño a la privacidad –y otros derechos fundamentales–, a pesar de que es valiosa para preservar la seguridad nacional. Y, en esa medida, el juez o la instancia de control debería adoptar medidas especiales de protección.

Ya antes se ha propuesto aplicar el principio de precaución a las tecnologías de la información y las comunicaciones (TIC). Som, Hilty y Thomas sugieren este enfoque para articular los riesgos y los beneficios de la tecnología en general. Las TIC, sostienen los autores, no solo pueden interactuar con prácticas sociales sino también cambiarlas. La incorporación de la tecnología es, simultáneamente, un proceso de causa y efecto. De allí deriva la potencialidad del riesgo. El objetivo, entonces, es preguntarse por las medidas de precaución que hubieran podido evitar efectos indeseados (Som, Hilty y Thomas 2004: 787, 799).

63 Cfr. Corte Constitucional, sentencia C-291 de 2007, M.P. Manuel José Cepeda.

64 Corte Constitucional, sentencia T-299 de 2008, M.P. Jaime Córdoba Triviño.

El efecto indeseado o el riesgo en nuestro caso es un marco legal y judicial que permita, e incluso incentive, el desarrollo de esquemas de vigilancia masiva, que son por naturaleza desproporcionados. Es decir, una vigilancia sin definiciones ni límites; sin controles adecuados; sin ponderación entre medios y fines. Una vigilancia que, en la práctica, derogue los derechos fundamentales.

Referencias

Cohen, J. 2012. *Configuring the Networked Self: Law, Code and the Play of Everyday Practice*. Yale University Press.

Cohen, J. 2000. "Examined Lives: Informational Privacy and the Subject as Object". *Stanford Law Review* 52: 1373.

Congreso de la República de Colombia, Ley 1453 de 2011, Medellín, junio 24; Ley 1581 de 2012, Bogotá, octubre 17; Ley Estatutaria 1621 de 2013, Bogotá, abril 17.

Congreso de los Estados Unidos Mexicanos, Ley de Seguridad Nacional, 31 de enero de 2005.

Congreso Nacional de Chile, Ley 19.974 de 2004, artículo 23.

Consejo Europeo, Directiva 2006/24/EC.

Convención Americana sobre Derechos Humanos, Pacto de San José, 7 al 22 de noviembre de 1969.

Corte Constitucional de Colombia, sentencias: T-444 de 1992, M.P. Alejandro Martínez Caballero; T-343 de 1993, M.P. Fabio Morón Díaz; C-179 de 1994, M.P. Carlos Gaviria Díaz; T-066 de 1998, M.P. Eduardo Cifuentes Muñoz; C-787 de 2004, M.P. Rodrigo Escobar Gil; C-591 de 2005, M.P. Clara Inés Vargas; C-291 de 2007, M.P. Manuel José Cepeda; C-336 de 2007, M.P. Jaime Córdoba Triviño; T-299 de 2008, M.P. Jaime Córdoba Triviño; T-708 de 2008, M.P. Clara Inés Vargas; T-1037 de 2008, M.P. Jaime Córdoba Triviño; C-131 de 2009, M.P. Nilson Pinilla Pinilla; T-298 de 2009, M.P. Luis Ernesto Vargas; C-334 de 2010, M.P. Juan Carlos Henao Pérez; C-913 de 2010, M.P. Nilson Pinilla Pinilla; C-540 de 2012, M.P. Jorge Iván Palacio Palacio.

Corte Europea de Derechos Humanos. Halford *vs*. Reino Unido, 1997.

Corte Europea de Justicia, Digital Rights Ireland Ltd (C-293/12) *vs.* Minister for Communications, Marine et ál., 8 de abril de 2014.

Cortés, C. 2014a. "La neutralidad de la red: la tensión entre la no discriminación y la gestión", en *Internet y derechos humanos. Aportes para la discusión en América Latina.* CELE, Universidad de Palermo.

Cortés, C. 2014b. "Vigilancia en la red: ¿qué significa monitorear y detectar contenidos en Internet?", en *Internet y derechos humanos. Aportes para la discusión en América Latina*. CELE, Universidad de Palermo.

Cortés, C. 2014c. "El deseo oficial de vigilar la red. Monitorear y detectar contenidos en Internet", en *Internet y derechos humanos. Aportes para la discusión en América Latina*. CELE, Universidad de Palermo.

Crocker, A. 2013. "Trackers that make phone calls: Considering First Amendment Protection for Location Data". *Harvard Journal of Law and Technology* 26 (2): 622.

Farahmand, F. y Q. Zhang. 2007. "Circuit Switching", en *The Handbook of Computer Networks* (vol. II).

Fowler, Alex. 2013. *Protecting our brand from a global spyware provider*. *Mozilla*. Recuperado de: https://blog.mozilla.org/blog/2013/04/30/protecting-our-brand-from-a-global-spyware-provider/ (consultado el 1 de abril de 2014).

Gallagher, Ryan. 2013. *Meet the machines that steal your phone's data. Arstechnica*. Recuperado de: http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/ (consultado el 2 de abril de 2014).

Hosein, G. y C. Wilson. 2013. "Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques". *Ohio State Law Journal* 74(6): 1071-1104.

Justice. 2011. *Freedom from Suspicion. Surveillance Reform for a Digital Age*. Londres: Justice.

Kang, J. 1998. "Information Privacy in Cyberspace". *Stanford Law Review* 50(4): 1260.

Kerr, O. 2004. "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution". *Michigan Law Review* 102: 107.

Landau, S. 2010. *Surveillance or Security?: The Risks Posed by New Wiretapping Technologies*. The MIT Press.

Mangakis, G. 2007. *Contra la censura. Ensayos sobre la pasión por silenciar*. Debate, editado por J.M. Coetzee.

Marquis-Boire, M. et ál. 2013a. *For Their Eyes Only. The Commercialization of Digital Spying*. Citizen Lab and Canada Centre for Global Security Studies, Munk School of Global Affairs, University of Toronto.

Marquis-Boire, M. et ál. 2013b. *You Only Click Twice: FinFisher's Global Proliferation*. Research Brief No. 15, marzo. The Citizen Lab, Munk School of Global Affairs, University of Toronto.

Mayer-Schönberger, V. y K. Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt.

Ministerio de las Tecnologías de la Información y las Comunicaciones, Decreto 1704 de 2012.

Naciones Unidas. 1966. Pacto Internacional de Derechos Civiles y Políticos.

Open Rights Group. 2013. *Digital Surveillance. Why the Snoopers' Charter is the wrong approach: A call for targeted and accountable investigatory powers*.

Oxford Pro Bono Publico. 2006. *Legal Opinion on Intercept Communication. The Justice Project*. Universidad de Oxford.

Pell, S. y C. Soghoian. 2012. "Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact". *Berkeley Technology Law Journal* 27: 117.

Poole, I. 2006. *Cellular Communications Explained. From Basics to 3G*. Newnes.

Som, C., L. Hilty y R. Thomas. 2004. "The precautionary principle in the information society". *Human and Ecological Risk Assesment* 10: 787-799.

Strobel, D. 2007. *IMSI Catcher*. Seminararbeit Ruhr-Universität Bochum.

Wu, T. 2010. *The Master Switch: The Rise and Fall of Information Empires*. Random House.

COLECCIÓN DOCUMENTOS DEJUSTICIA

• DOCUMENTOS 1

ETNORREPARACIONES: la justicia colectiva étnica y la reparación a pueblos indígenas y comunidades afrodescendientes en Colombia

Publicación digital e impresa

César Rodríguez Garavito, Yukyan Lam

2011

• DOCUMENTOS 2

LA CONSULTA PREVIA: DILEMAS Y SOLUCIONES. Lecciones del proceso de construcción del decreto de reparación y restitución de tierras para pueblos indígenas en Colombia

Publicación digital e impresa

César Rodríguez Garavito, Natalia Orduz Salinas

2012

• DOCUMENTOS 3

LA ADICCIÓN PUNITIVA: La desproporción de leyes de drogas en América Latina

Publicación digital e impresa

Rodrigo Uprimny, Diana Esther Guzmán, Jorge Parra Norato

2012

• DOCUMENTOS 4

ORDEN PÚBLICO Y PERFILES RACIALES: experiencias de afrocolombianos con la policía en Cali

Publicación digital e impresa

Yukyan Lam, Camilo Ávila

2013

• DOCUMENTOS 5

INSTITUCIONES Y NARCOTRÁFICO: la geografía judicial de los delitos de drogas en Colombia

Publicación digital

Mauricio García Villegas, Jose Rafael Espinosa Restrepo, Felipe Jiménez Ángel

2013

• DOCUMENTOS 6

ENTRE ESTEREOTIPOS: Trayectorias laborales de mujeres y hombres en Colombia

Publicación digital

Diana Esther Guzmán, Annika Dalén

2013

• DOCUMENTOS 7

LA DISCRIMINACIÓN RACIAL EN EL TRABAJO: Un estudio experimental en Bogotá

Publicación digital e impresa

César Rodríguez Garavito, Juan Camilo Cárdenas C., Juan David Oviedo M., Sebastián Villamizar S.

2013

COLECCIÓN DOCUMENTOS DEJUSTICIA

• DOCUMENTOS 8

LA REGULACIÓN DE LA INTERRUPCIÓN VOLUNTARIA DEL EMBARAZO EN COLOMBIA

Publicación digital

Annika Dalén, Diana Esther Guzmán, Paola Molano

2013

• DOCUMENTOS 9

ACOSO LABORAL

Publicación digital

Diana Guzmán, Annika Dalén

2013

• DOCUMENTOS 10

ACCESO A LA JUSTICIA: Mujeres, conflicto armado y justicia

Publicación digital

Diana Esther Guzmán Rodríguez, Sylvia Prieto Dávila

2013

• DOCUMENTOS 11

LA IMPLEMENTACIÓN DE LA DESPENALIZACIÓN PARCIAL DEL ABORTO

Publicación digital e impresa

Annika Dalén

2013

• DOCUMENTOS 12

RESTITUCIÓN DE TIERRAS Y ENFOQUE DE GÉNERO

Publicación digital e impresa

Diana Esther Guzmán, Nina Chaparro

2013

• DOCUMENTOS 13

RAZA Y VIVIENDA EN COLOMBIA: la segregación residencial y las condiciones de vida en las ciudades

Publicación digital e impresa

María José Álvarez Rivadulla, César Rodríguez Garavito, Sebastián Villamizar Santamaría, Natalia Duarte

2013

• DOCUMENTOS 14

PARTICIPACIÓN POLÍTICA DE LAS MUJERES Y PARTIDOS. Posibilidades a partir de la reforma política de 2011.

Publicación digital

Diana Esther Guzmán Rodríguez, Sylvia Prieto Dávila

2013

• DOCUMENTOS 15

BANCADA DE MUJERES DEL CONGRESO: una historia por contar

Publicación digital

Sylvia Cristina Prieto Dávila, Diana Guzmán Rodríguez

2013

COLECCIÓN DOCUMENTOS DEJUSTICIA

• DOCUMENTOS 16

OBLIGACIONES CRUZADAS: Políticas de drogas y derechos humanos

Publicación digital

Diana Guzmán, Jorge Parra, Rodrigo Uprimny

2013

• DOCUMENTOS 17

GUÍA PARA IMPLEMENTAR DECISIONES SOBRE DERECHOS SOCIALES

Estrategias para los jueces, funcionarios y activistas

Publicación digital e impresa

César Rodríguez Garavito, Celeste Kauffman

2014