DERECHOS DIGITALES
América Latina

RETENCIÓN DE DATOS Y REGISTRO DE TELÉFONOS MÓVILES

CHILE EN EL CONTEXTO LATINOAMERICANO

MARIANNE DÍAZ

RETENCIÓN DE DATOS Y REGISTRO DE TELÉFONOS MÓVILES

CHILE EN EL CONTEXTO LATINOAMERICANO

MARIANNE DÍAZ

Portada:Violeta Cereceda
Diagramación: Constanza Figueroa.
Edición y correcciones: Vladimir Garay.
Junio 2017.

Este informe fue realizado por Derechos Digitales, con el financiamiento de Privacy International y Ford Foundation. Derechos Digitales es una organización independiente y sin fines de lucro, fundada en el año 2005 y cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en el entorno digital, desde el interés público. Entre sus principales ejes de interés está la defensa y promoción la libertad de expresión, el acceso a la cultura y la privacidad.

Resumen [1]

Las medidas de retención de datos y registro de teléfonos móviles constituyen restricciones a los derechos fundamentales a la privacidad y a la libertad en las comunicaciones. Como tales, deben cumplir con una serie de requisitos mínimos que garanticen el respeto a los estándares internacionales en materia de derechos humanos. Frente a la tendencia regional y global que lleva a gobiernos y a proveedores de servicio a acumular una cantidad cada vez mayor de información sobre sus usuarios, este estudio intenta una aproximación comparada a la manera en que las legislaciones de México, Brasil, Colombia, Perú, Argentina y Chile abordan la retención de datos y el registro de teléfonos móviles, de cara a sus obligaciones y compromisos internacionales en el marco interamericano, y en particular en relación a los proyectos legislativos que en Chile buscan realizar cambios al actual marco regulatorio de las telecomunicaciones.

Palabras clave: Retención de datos, privacidad, comunicaciones, registro de SIM, telefonía móvil.

1 La autora agradece a Valentina Hernández y Paula Jaramillo la información suministrada para la elaboración de esta investigación.

Contenido

Resumen ejecutivo

Este reporte es el resultado de un examen la legislación vigente en materia de retención de datos y registro de teléfonos móviles en Argentina, Brasil, México, Perú y Chile (con énfasis en este último), en relación con los principios y parámetros de derechos humanos que rigen las restricciones en el acceso a las comunicaciones y la libertad de expresión.

Al mismo tiempo que existe una tendencia global de las naciones por regular las telecomunicaciones de modo más estricto, bajo la justificación de combatir el terrorismo y el crimen organizado, el impulso en respuesta apunta a señalar que los usos de la tecnología con fines de comunicación constituyen usos protegidos por los estándares internacionales de derechos humanos. Como ejemplo, el anonimato, que suele ser presentado por los estados como un factor peligroso que debe ser combatido, dando por sentado que coadyuva a la perpetración de crímenes, es visto por Naciones Unidas como una garantía a la libertad de expresión y al libre flujo de ideas en el contexto de una sociedad.

En el balance de esta tensión, la Convención Americana sobre Derechos Humanos contempla los requisitos mínimos que debe contener cualquier restricción a la libertad de expresión en la región. Aceptamos, así, que existen limitaciones y que es potestad de los estados regular los casos en los que se requiere restringir estos derechos, pero postulamos que dichas medidas deben cumplir con cinco requisitos: (1) legalidad, (2) búsqueda de una finalidad imperativa, (3) necesidad, idoneidad y proporcionalidad de la medida en relación con el fin perseguido, (4) garantías judiciales, y (5) satisfacción del debido proceso.

Así, observamos que las legislaciones latinoamericanas en materia de retención de datos y registro de tarjetas SIM resultan inconsistentes en el cumplimiento de estos parámetros. En varios casos, las medidas son tomadas sorteando el principio de legalidad, a través de una orden ejecutiva, poniendo en riesgo garantías mínimas del sistema democrático. En otros, se permite el acceso por parte de los órganos públicos a los datos sin la garantía de una orden judicial, lo cual violenta el debido proceso y ubica a los ciudadanos en un estado de indefensión que afecta gravemente sus derechos humanos. Como se relata, una tendencia reciente ha incluido mecanismos de registro sobre uno de los números que identifica a cada teléfono móvil, como el denominado IMEI.

Resulta patente, con la evidencia que tenemos disponible, que medidas como el registro obligatorio de tarjetas SIM son no solo desproporcionadas, sino directamente inútiles. Sus ventajas alegadas han demostrado no tener fundamentos en la realidad, luego de la aplicación en diversos países, en especial en la región africana. Asimismo, tanto el registro obligatorio de tarjetas SIM como las medidas de retención de datos que carecen de estándares mínimos contribuyen a profundizar una relación de desequilibrio de poder entre los usuarios, las compañías de telefonía móvil y los estados, un desequilibrio que afecta la capacidad de los ciudadanos para exigir el cumplimiento de sus derechos fundamentales. Partiendo de este análisis, elaboramos una serie de recomendaciones, no solo al Estado chileno, sino a los estados en general, con miras a lograr este balance.

1. Registro de teléfonos móviles y retención de datos: alcance y propósito

La seguridad nacional y la prevención y persecución del crimen son los argumentos más frecuentemente empleados para justificar la creciente vigilancia a las comunicaciones, incluyendo la acumulación de datos sobre esas comunicaciones. Durante las últimas dos décadas, una marcada tendencia global apunta a la expansión y puesta en práctica de normativas prescriptivas que obligan al requerimiento y retención de una mayor cantidad de datos al usuario de teléfonos móviles por parte de las compañías prestadoras del servicio (Gow y Parisi, 2008). La ola de implementación de registros obligatorios de tarjetas SIM se inicia en 2003, con las normativas de Brasil, Alemania y Suiza (GSMA, 2013) y para 2016 alrededor de 90 países requerían registro obligatorio a los usuarios de tarjetas SIM (GSMA, 2016).

En su mayoría, las autoridades que implementan estas medidas emplean como justificación la necesidad de utilizar la información como una herramienta en la lucha contra el terrorismo y el crimen organizado (Kapellmann y Reyes, 2015). También, aunque en menor medida, son empleados como argumentos el combate al robo y hurto de dispositivos móviles, así como la necesidad de disminuir la pérdida de recursos en la movilización del personal de policía y servicios de emergencia en casos de llamados de broma (Eagle News, 2016).

El mercado de la telefonía prepagada conforma un alto porcentaje de la totalidad del mercado móvil, alcanzando hasta el 90 % en países como México (Gow y Parisi, 2008). Esto implica que, si bien en el momento de mayor auge de la creación de estas medidas, ya planteaban conflictos en relación con la cantidad de datos personales acumulados y manejados como consecuencia de ellas, el alza porcentual en el uso de telefonía prepagada, sumada al avance de la tecnología que lleva al crecimiento en el número de funciones que estos dispositivos pueden cumplir, permite acumular un número mucho mayor de datos, no solo de la comunicación propiamente dicha, sino de la ubicación del usuario, de su historial de navegación y un sinnúmero de otros puntos de información.

A pesar de la amplitud con la cual este tipo de medidas sigue siendo implementadas hoy en día, existe también evidencia de su eliminación en algunos países. La aplicación efectiva de estas medidas en diversos países del globo ha demostrado la inexistencia de un vínculo claro entre las medidas de registro obligatorio y la prevención del terrorismo o del crimen organizado (Privacy International, 2004). En el caso latinoamericano, México modificó en 2009 su legislación procesal penal nacional y de telecomunicaciones, con la finalidad de establecer la creación del Registro Nacional de Usuarios de Telefonía Móvil (RENAUT), el cual obligaba a que los proveedores de servicios de telecomunicaciones llevaran un registro en el cual cada teléfono celular estuviera asociado de manera clara a un ciudadano, siendo este registro accesible a petición del Ministerio Público, que tendría acceso a datos como la geolocalización del dispositivo o el contenido de las comunicaciones. Sin embargo, estas disposiciones se derogaron apenas tres años después, puesto que, en lugar de disminuir, el porcentaje de comisión de los delitos en cuestión aumentó dentro de la vigencia del régimen (GSMA, 2013).

Del mismo modo, un estudio hecho por en 32 países de África subsahariana (Jentzsch, 2012) muestra que el registro obligatorio de tarjetas SIM no solo deprime el crecimiento en el uso de telefonía móvil

(un efecto indeseable en países que buscan incrementar sus tasas de acceso a las telecomunicaciones) sino que no existe evidencia convincente de que la implementación de dicho registro disminuya las tasas delictivas.

Asimismo, la implementación de registros de usuarios, o de datos o metadatos de comunicaciones no está exentas de fallos. En muchas ocasiones, los mandatos de retener datos no van acompañados de estándares claros respecto al manejo, almacenamiento y eliminación segura de esos datos, que combinados, pueden revelar detalles altamente específicos sobre la vida privada de cualquier individuo particular, incluyendo aspectos médicos, financieros y familiares (Keane, 2015).

En consecuencia, el registro y retención de la información asociada a las comunicaciones móviles plantea una serie de consideraciones en torno a la privacidad y la intimidad de los ciudadanos, quienes pueden verse afectados por diversos factores: la adquisición, manejo y almacenamiento de los datos, las posibilidades de los ciudadanos de controlar la información que sobre ellos exista en manos de terceros, y la seguridad y protocolos en torno al procesamiento de dicha información (Kapellmann y Reyes, 2015).

Tal como ha planteado el Relator de Naciones Unidas para la Libertad de Expresión (Kaye, 2015), el registro obligatorio de tarjetas SIM puede proporcionar a los gobiernos la capacidad de monitorear el comportamiento de los individuos más allá de sus intereses legítimos, así como poner trabas al acceso a herramientas de comunicación que alejan a los ciudadanos del ejercicio de sus derechos fundamentales.

Vale considerar, por ejemplo, que exigir documentos de identidad o evidencia de una dirección permanente puede dificultar el acceso a las telecomunicaciones a personas pertenecientes a grupos marginalizados: personas de bajos ingresos, inmigrantes, mujeres en situaciones precarias, personas transgénero, entre otros ejemplos. Igualmente, la existencia de un registro de telefonía móvil incrementa los costos de cambiar de proveedor para el usuario, ya que tendrá que registrarse nuevamente con un nuevo proveedor, lo que a su vez tiene un impacto en la privacidad. A mayor fidelidad con un determinado proveedor, el perfil personal de este usuario se vuelve más detallado (Jentzsch, 2012). Todos estos aspectos presentan implicaciones en cuanto al ejercicio ciudadano de los derechos humanos en el contexto de las comunicaciones móviles.

La Convención Americana contempla los requisitos mínimos que debe contener cualquier restricción a la libertad de expresión, que deben ser evaluados de manera sistémica, pero que en concreto son cinco: (1) legalidad, (2) búsqueda de una finalidad imperativa, (3) necesidad, idoneidad y proporcionalidad de la medida en relación con el fin perseguido, (4) garantías judiciales, y (5) satisfacción del debido proceso. Estos mismos estándares se encuentran desarrollados en los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, elaborados con el consenso de la sociedad civil para determinar la legitimidad de las medidas de vigilancia en el contexto de las comunicaciones. Partiendo de estos parámetros se busca poner límites a la situación natural de desigualdad en la relación de poder que surge entre el Estado y los proveedores de servicio, por un lado, y los usuarios, por el otro.

2. Generalidades

2.1. Retención de datos de comunicaciones

A pesar de que las prácticas de retención de datos en materia de telecomunicaciones se han vuelto ubicuas en los últimos años, los estándares de derechos humanos con respecto a la captura de datos relacionados con las comunicaciones establecen que cualquier práctica de esta índole constituye potencialmente una interferencia al derecho a la privacidad, y que esto se aplica a la retención de datos de las telecomunicaciones independientemente de que dichos datos sean posteriormente consultados o usados. El dato, como unidad mínima de información, puede no poseer o aportar una gran cantidad de significado por sí mismo, pero cobra un enorme sentido al ser correlacionado con otros puntos de información que, sumados, construyen un perfil del usuario, de sus redes interpersonales y de su comportamiento en la sociedad y en el mercado.

Tal como ha reconocido el Consejo de Derechos Humanos de la ONU (UNHRC, 2014) la mera posibilidad de que la información relativa a las comunicaciones sea capturada interfiere con el derecho a la privacidad y potencialmente tiene un efecto silenciador sobre la libertad de expresión. En este sentido, corresponde a los estados demostrar que estas interferencias cumplen con los requisitos mínimos, es decir, que no son arbitrarias ni desproporcionadas. En el contexto del Sistema Interamericano de Derechos Humanos, las medidas que afectan o restringen las comunicaciones deben ser armonizadas con los estándares internacionales, por cuanto afectan derechos fundamentales. La retención de datos obligatoria por parte de terceros, en la que los gobiernos requieren que las compañías telefónicas y los proveedores de servicios de internet almacenen los datos y metadatos relativos a las comunicaciones de sus clientes no es considerada por Naciones Unidas como necesaria o proporcional.

Existe consenso en la sociedad civil en cuanto a que la retención de datos a priori nunca debería ser requerida a los proveedores de servicio, por cuanto vulnera el derecho de los individuos a expresarse de manera anónima (Privacy International, Access Now, y Electronic Frontier Foundation, 2014). Así hemos visto, por ejemplo, que en 2014 el Tribunal de Justicia de la Unión Europea declaró inválida la directiva sobre conservación de datos, normativa que buscaba armonizar las disposiciones de los estados miembros con respecto a la conservación de datos generados o tratados por los proveedores de los servicios de telecomunicaciones. El TJUE consideró en tal ocasión que "al imponer la conservación de estos datos y al permitir el acceso a las autoridades nacionales competentes", la Directiva constituía una intrusión grave e indebida en los derechos fundamentales al respeto de la vida privada y a la protección de datos de carácter personal. Al evaluar la Directiva, el TJUE tomó en consideración el hecho de que esta: 1) abarcaba a todas las personas, medios de comunicación y datos sin ninguna diferenciación, limitación o excepción, 2) no fijaba criterios que permitieran garantizar que únicamente las autoridades competentes podrían tener acceso a los datos y que estos serían usados para prevenir, detectar o reprimir delitos cuya gravedad justificara la injerencia, y 3) la Directiva fijaba un período de conservación de datos de entre seis y veinticuatro meses, sin precisar cuáles criterios deberían emplearse para determinar el período y así garantizar que este se limitara al tiempo estrictamente necesario. Estos factores llevaron al Tribunal europeo a considerar que la Directiva no poseía garantías suficientes

que permitan asegurar la protección de los datos de los ciudadanos contra accesos y usos ilícitos, y contra los posibles abusos por parte de las autoridades o de los intermediarios (Tribunal de Justicia de la Unión Europea, 2014).

De igual modo, en 2014 el Senado paraguayo inició la discusión de un proyecto de ley (popularmente conocido como «Pyrawebs») que obligaría a los proveedores de servicio de internet a conservar los datos de las comunicaciones de sus usuarios por doce meses, así como el acceso a estos datos por parte de las autoridades mediante una orden judicial. Los datos a ser recabados incluían detalles como la duración de la conexión, la identidad de las partes y la geolocalización de los usuarios (Sequera, Alonso y Rodríguez, 2014). La organización paraguaya TEDIC impulsó una campaña que tuvo como centro el argumento de que la retención de datos obligatoria es una medida desproporcionada e invasiva, que crea enormes potenciales para el abuso por parte de empresas y gobiernos, y constituye una infracción grave a los derechos fundamentales de las personas. Finalmente, el proyecto de ley fue rechazado tanto en la Cámara de Diputados como en el Senado (Flores, 2015).

2.2. Registro de teléfonos móviles

2.2.1. Registro de SIM

Para efectos de la presente investigación, denominamos registro obligatorio de SIM a todo procedimiento en el que los individuos deban pasar a través del proceso de registrar una tarjeta SIM (subscriber identity model) para su teléfono móvil usando su nombre (Jentzsch, 2012). Una tarjeta SIM almacena la clave de servicio del suscriptor (IMSI, por sus siglas en inglés), que se utiliza para identificar a un determinado usuario. La tecnología de una tarjeta SIM permite que un usuario cambie de dispositivo simplemente al removerla de un teléfono e insertarla en otro, sin necesidad de cambiar nada más, y contiene un serial único, la clave de suscriptor (IMSI), así como información de autenticación y cifrado, información temporal relativa a la red, y dos contraseñas de identificación y bloqueo (PIN y PUK) (Aririguzo y Agbaraji, 2016).

El registro obligatorio de tarjetas SIM es empleado para asociar un determinado microchip con un usuario específico e identificado con precisión. Este tipo de procedimiento es similar a los procedimientos KYC ("Conoce a tu cliente") aplicados por entidades bancarias para prevenir actividades de lavado de dinero. Los procesos de este tipo se caracterizan por recabar una cierta cantidad de información relativa a la identidad de una persona y posiblemente contrastar esta información contra una lista total o parcial, por ejemplo, una lista de personas políticamente expuestas, personas con antecedentes penales o directamente contra la base de datos de ciudadanos registrados como residentes legales de un determinado país.

El registro obligatorio de tarjetas SIM suele tener por finalidad principal la regulación y control de las transacciones anónimas. En general, los organismos dedicados al cumplimiento de la ley tienden a mostrar preocupación acerca del vínculo aparente entre el mercado anónimo de telefonía móvil prepagada y las actividades criminales y terroristas (Gow y Parisi, 2008). No obstante, la existencia real de este vínculo es dudosa, siendo el caso que dos tercios de los terroristas operan bajo su identidad real, y el 80% de los países que han sido más afectados por actividades terroristas ya tienen sistemas nacio-

nales de identidad (un tercio de los cuales utiliza incluso tecnologías biométricas). No existe evidencia alguna de que la implementación de dichos sistemas nacionales de identidad haya tenido ningún tipo de influencia sobre la actividad terrorista (Privacy International, 2004).

En países como Canadá, donde la recolección de información de carácter personal por parte de un proveedor de servicio está sujeta a una prueba de oportunidad razonable, requerir la verificación de identidad por parte de las empresas de telecomunicaciones es considerado una invasión de la privacidad, dado que dicha información no es necesaria para prestar el servicio y en consecuencia, se considera que no es ni razonable ni apropiado requerirla (Gow y Parisi, 2008). Algunos investigadores han alegado que la obligatoriedad del registro de tarjetas SIM no solo constituiría una invasión ilegítima a la privacidad de los usuarios, sino que afectaría de manera especial a un sector específico de la población que acude al mercado de tarjetas prepagadas por una serie de razones, entre ellas, la falta de crédito financiero.

El argumento central para implementar el registro de tarjetas SIM y la recolección de información personal como consecuencia de este, es que dicha práctica ayudaría a la lucha contra el terrorismo, al dificultar el anonimato de las personas. Por un lado, la falta de correlación entre los sistemas de identificación obligatoria y la prevención del terrorismo ha quedado demostrada desde hace mucho tiempo (Privacy International, 2004); por otra parte, diversos investigadores han expuesto el argumento de que, ante un escrutinio más cercano de la noción de "anonimato", resulta claro que esta condición no es un absoluto, sino un espectro. Wallace (1999) define el anonimato como la imposibilidad de coordinar las características de una persona con la finalidad de establecer su identidad. Por su parte, Gary Marx (1999) ha descrito siete categorías de características de identidad:

- Nombre legal
- Ubicación
- Seudónimos rastreables
- Seudónimos no rastreables
- Patrones de comportamiento
- Atributos sociales o físicos
- Símbolos de elegibilidad/no-elegibilidad

En este sentido, y siguiendo a Gow y Parisi, en un contrato prepago anónimo, el número de teléfono sirve como "identificador opaco", que puede ser usado para rastrear las llamadas y efectuar los pagos, proporcionando así un mecanismo de anonimato sumamente limitado, al convertirse en una pieza de información central para coordinar otros rasgos que permitan determinar la identidad del usuario. El anonimato, si bien central a la noción misma de privacidad y de libertad de expresión (Kaye, 2015), no es un estado absoluto que sea alcanzable para un usuario de telefonía móvil. Aun en el escenario ideal (un cliente activa una línea prepagada utilizando dinero en efectivo), se mantienen varias de las condiciones señaladas por Wallace para determinar la identidad del usuario. Incluso un identificador opaco, como el número telefónico de un usuario, proporciona la posibilidad de generar al menos tres piezas de información para la determinación de la identidad.

La noción de que recabar un número mayor de piezas de información en torno a la actividad telefónica de los usuarios contribuiría a combatir el crimen parte del principio erróneo de que las personas

que eligen involucrarse en actividades criminales harían esto utilizando líneas telefónicas registradas a su nombre. En la realidad, lo más probable es que los criminales adopten una táctica alternativa, ya sea clonar ilícitamente las tarjetas SIM de terceros, utilizar SIMs extranjeras en modalidad de roaming o adoptar tecnologías de telefonía satelital y de internet (Donovan & Martin, 2014).

Dado que este supuesto es falso, la implementación de mecanismos de registro de tarjetas SIM suele traducirse en conductas que comprometen la privacidad de ciudadanos cuyas actividades son legales, afectando así sus libertades básicas a través de un efecto de enfriamiento de la libertad de expresión (Donovan y Martin, 2014). En particular, la obligatoriedad del registro de tarjetas SIM vulnera todo potencial de ejercicio del anonimato, una restricción que disuade el libre flujo de ideas y de información (OHCHR). De acuerdo con los Principios sobre Vigilancia de las Comunicaciones, este tipo de medidas aplicadas a la población en general no resultan proporcionales a los principios internacionales en materia de derechos humanos, en especial el derecho a expresarse anónimamente, y los Estados deberían evitar exigir la identificación de los usuarios de telefonía móvil.

No obstante ello, diversos países de Latinoamérica poseen normativa que exige o busca exigir la creación de registros obligatorios de tarjetas SIM, información que se une a los ya existentes datos que las compañías de telecomunicaciones retienen por orden de ley para identificar e individualizar a los usuarios ante las autoridades.

2.2.2. Registro de IMEI

El IMEI (International Mobile Equipment Identity) es un número conformado por quince dígitos decimales que permiten identificar la marca y modelo de un dispositivo móvil, así como su número serial. A través del código IMEI, un operador móvil puede rastrear la utilización de un dispositivo específico con mucha rapidez, si es usado en la misma red móvil (Aririguzo y Agbaraji, 2016).

El registro de IMEI se lleva a cabo a través de la recopilación de información de cada dispositivo móvil activo, mediante la inclusión en una base de datos tanto del número IMEI como de información específica sobre el usuario que posee el dispositivo. El principal argumento empleado para defender la imposición de medidas de registro obligatorio de IMEI suele ser la persecución del delito de robo de teléfonos. Así, al saber el número IMEI de un dispositivo que ha sido robado, las operadoras pueden rastrear sus redes e identificar a la persona que podría estar usando el dispositivo, junto a la tarjeta SIM que está siendo usada, y pueden también bloquear el acceso de dicho usuario al sistema, ya sea por medio del bloqueo de la tarjeta SIM (que impide que la línea siga siendo utilizada) o a través del bloqueo del código IMEI (que deshabilita por completo el dispositivo para su uso con cualquier tarjeta SIM). Quienes proponen esta medida sostienen que la implementación del registro de IMEI no solo combatiría la venta de teléfonos robados, sino que ayudaría a combatir otros crímenes, como los secuestros.

A grandes rasgos, el sistema de registro de IMEI funciona mediante uno de dos modelos posibles: en el sistema de "lista blanca", los clientes pueden usar sus dispositivos solo si han sido registrados con la compañía de telecomunicaciones; si no están registrados, las compañías deberán negar el servicio hasta que lo estén.

En el sistema de "lista negra", los dispositivos son considerados legítimos por defecto, con la excepción

de aquellos que aparezcan en la lista. Ésta consiste en un registro de los IMEIs asociados con dispositivos móviles a los cuales debe negarse servicio, ya que han sido reportados como perdidos o robados. Para que este sistema funcione, la lista debe estar centralizada a través de las diferentes operadoras, de modo que aquellos dispositivos que hayan sido reportados no funcionen en ninguna de las diferentes redes (GSMA, 2017).

La implementación de un sistema de registro de IMEI bajo el modelo de lista blanca por lo general implica, además, la entrada en vigencia de un lapso moratorio para el registro de los dispositivos que se encuentran en funcionamiento previamente a la promulgación de la ley. Esto significa que se instaura una fecha de corte (o "apagón") a partir de la cual todos los dispositivos que no hayan sido registrados son desconectados del servicio. Esta medida puede ocasionar riesgos graves a los derechos humanos; por ejemplo, en Kenia, en 2012, las autoridades desconectaron las líneas telefónicas de alrededor de 1.5 millones de ciudadanos, dado que los códigos IMEI de sus dispositivos no se encontraban en la base de datos internacional. En este caso, la medida buscaba combatir la venta de teléfonos falsificados (copias de marcas y modelos populares elaborados con materiales baratos), con el fin de "proteger a los consumidores de teléfonos inferiores, resguardar los sistemas de pago móvil y prevenir el crimen" (Chebusiri, 2012).

A través de la aplicación de esta medida, cientos de miles de personas vieron afectadas no solo sus capacidades de comunicarse libremente, sino también su único medio de acceder y participar en la economía, ya que para muchas el teléfono móvil era su único mecanismo para comunicarse con clientes, acceder a internet e incluso realizar pagos a través de transferencias. Refiriéndose al caso de Kenia, la organización internacional Artículo 19 señaló que la medida era desproporcionada y que, en consecuencia, fallaba la prueba con respecto a los principios de necesidad, proporcionalidad y legalidad, en particular porque era posible alcanzar el mismo fin a través de otras medidas:

Muchos de quienes usan dispositivos "falsificados", particularmente suscriptores pobres que viven en la periferia y en áreas rurales, no están al tanto de que sus dispositivos son falsificados. La mayoría de ellos no puede distinguir la diferencia de un artículo genuino, y muchos de ellos los compran de distribuidores registrados, bajo la presunción de que el producto es genuino. Algunos podrían no tener la capacidad de comprar o cambiar su dispositivo debido a los costos prohibitivos asociados con nuevas compras o cambios (Artículo 19, 2011).

En la mayoría de los países predomina el sistema de lista negra para el registro de IMEI. En Guatemala, por ejemplo, se creó en 2013 la Ley de Equipos Terminales Móviles (Decreto 8-2013), que estableció la obligación por parte de las empresas operadoras de telefonía móvil de dar de baja las líneas que los usuarios no hubieran registrado en un plazo de tres años, que se cumplió el 8 de octubre de 2016. La norma contempla de manera simultánea un registro de tarjetas SIM (que incluye todos los datos personales básicos del cliente) y un registro de IMEI en base al sistema de lista negra (denominado en la ley "Base de Datos Negativa"), contentiva de la información de IMEI de los equipos móviles que han sido denunciados como robados, hurtados o extraviados. Otros países han adoptado sistemas de lista blanca parcial o fragmentada: en Ecuador, desde 2014, es obligatorio que todos los teléfonos móviles que ingresen al país por vía aérea sean registrados en una base de datos llevada por la Superintendencia de Telecomunicaciones del Ecuador (Supertel) y el Servicio Nacional de Aduana del Ecuador (Senae). Para que un dispositivo pueda

ser registrado, la marca y modelo debe estar homologada en el Ecuador y no estar reportado por robo en Ecuador, Colombia, Perú y Bolivia (El Mercurio, 2014).

3. Colombia

3.1. Retención de datos

En Colombia, el Decreto 1704 rige la medida de retención de datos de las comunicaciones en el contexto de la investigación criminal, mientras la Ley 1621 de 2013 hace lo propio con respecto a actividades de inteligencia.

El Decreto 1704 exige a los proveedores de servicio conservar la información de las comunicaciones de sus clientes que permita saber su geolocalización en tiempo real. Por su parte, la Ley 1621 exige retener el historial de comunicaciones de los usuarios, los datos técnicos de identificación de los suscriptores que forman parte de la comunicación y los datos de geolocalización. En ambos casos, los datos deben ser conservados por un lapso de cinco años, y en ambos casos la redacción del texto legal es vaga e imprecisa, abriendo dudas sobre qué significa "el historial de comunicaciones", o si la obligación de retener datos se extiende también a los datos derivados de la navegación en internet. La Ley 1704 habla de datos de geolocalización, expresándolo como "información específica contenida en sus bases de datos, tal como sectores, coordenadas geográficas y potencia", dejando abiertas las posibilidades de interpretación a las autoridades o a las empresas de telecomunicaciones.

3.2. Registro de teléfonos móviles

El Decreto Nº 1630, de mayo de 2011, crea un registro nacional de teléfonos móviles, a través de la adopción de dos bases de datos. La base de datos negativa contiene los IMEI de los dispositivos que hayan sido reportados como hurtados o extraviados, tanto en Colombia como en el extranjero, mientras que la base de datos positiva incluye los equipos móviles ingresados o fabricados legalmente en territorio colombiano. Esta última conecta el IMEI con la identidad del usuario, a quien se exige que entregue a las operadoras de telecomunicaciones su nombre completo, tipo y número de documento de identidad, su dirección y su número telefónico. Las operadoras están obligadas a verificar esta información contra diferentes bases de datos, incluyendo la base de datos nacional de documentos de identidad, el registro del estado civil y bases de datos de historial crediticio (Privacy International, 2017).

En el caso colombiano, a pesar de que no existe registro obligatorio de tarjetas SIM, las IMEI se encuentran asociadas con un usuario específico. Aunado a ello, para garantizar que todas las IMEI legítimas estén registradas en la base de datos positiva, se implementó un sistema de verificación que exige a los proveedores del servicio detectar y registrar cada IMEI que genere actividad en sus redes, lo cual se lleva a cabo a través de un análisis de metadatos denominado CDR. La información recogida y analizada incluye los códigos IMSI e IMEI, la fecha, hora y características de la actividad, y la coherencia de estos datos. Posteriormente a este análisis, todos los IMEI considerados como "irregulares" son bloqueados.

La creación del registro de IMEI ha sido objeto de críticas dentro de Colombia, pues organizaciones de la sociedad civil consideran excesiva la cantidad de información que se requiere para elaborar la

base de datos positiva, amén de los posibles riesgos en el manejo de esos datos. Además, la homologación de equipos previos al registro y adquiridos en el extranjero ha dado origen a un sinfín de inconvenientes: al principio, se requería un pago que dejaba la opción fuera del alcance de la mayoría de las personas y, posteriormente, aunque este requisito fue eliminado, el procedimiento de registro seguía requiriendo un nivel de conocimientos técnicos que afectaba al usuario común. Con posterioridad a esto, el procedimiento fue nuevamente modificado para facilitar el acceso a la población en general (Sáenz, 2016).

4. Brasil

4.1. Retención de datos

La agencia brasileña de telecomunicaciones, ANATEL, exige a los ISP retener los registros de conexiones por el plazo de un año. Este requerimiento se ve ratificado por la ley N° 12.965/24, comúnmente conocida como Marco Civil de Internet, que establece que

> al proveer una conexión de internet, el sistema proveedor independiente que corresponda tiene el deber de almacenar los registros de conexión, en confidencialidad y en un ambiente seguro y controlado, por el periodo de un año, conforme a la normativa vigente. Los registros de conexión conforman el conjunto de datos concernientes a la fecha y hora de comienzo y fin de una conexión a internet, su duración y la dirección IP usada por la terminal para enviar y recibir paquetes de datos.

La misma normativa, en su artículo 15, establece la obligación de los proveedores de servicio de mantener los registros de acceso a las aplicaciones de internet en confidencialidad y en un ámbito controlado y seguro, por seis meses. Tanto este período como el mencionado anteriormente pueden ser extendidos por medio de mociones cautelares, sin que ninguna norma establezca cuál es el lapso máximo para tal extensión. Al mismo tiempo, los proveedores de servicios de conexión de internet son requeridos por la resolución 614/13 a retener los registros de conexión y los datos de cuenta de sus suscriptores por al menos un año.

Por otra parte, los requisitos a los proveedores de telefonía fija y móvil son aún mayores, siendo que las resoluciones 426/05 y 477/07 establecen que estos deben mantener a disposición de ANATEL y otros interesados, los datos de registros telefónicos, por un lapso de al menos cinco años, sin indicar un tope máximo para la retención. En el caso de la telefonía fija, no queda claro cuáles datos están incluidos en el concepto de "registro telefónico", mientras que en lo que respecta a la telefonía móvil, la normativa se refiere a los datos sobre llamadas entrantes y salientes, fecha, hora, duración, precio e información de cuenta de los suscriptores.

Estos registros de llamadas, de acuerdo con lo establecido por la Ley de Organizaciones Criminales en su artículo 17, deben ser mantenidos a disposición de las autoridades por el período ya mencionado.

4.2. Registro de teléfonos móviles

La ya mencionada Resolución 477/07 establece requisitos mínimos en cuanto a los datos personales que los usuarios deben proporcionar para contratar un servicio de telefonía móvil: su nombre, su número de documento de identidad, su número de identificación fiscal y su dirección. En 2016, este requisito se ve reforzado por la adopción de la Ley Nº 16.269, del 5 de julio de 2016, que establece la obligatoriedad del registro de tarjetas SIM al momento de su venta, registro que debe contener el nombre completo de quien la adquiere, su dirección, su número de documento de identidad y de identificación fiscal y el número de autenticación del chip, siendo que todos estos datos deben ser

verificados mediante la presentación de documentos oficiales, de los cuales el proveedor del producto deberá conservar una copia.

Si bien los datos que exige esta ley son los mismos mencionados en la resolución 477/07, la principal diferencia radica en que la Ley Nº 16.269 establece sanciones hasta por el monto de 10.000 unidades fiscales, e inclusive la incautación del inventario de productos disponibles del proveedor al momento de la aplicación de la sanción, en caso de reincidencia.

La Ley Nº 16.269 fue presentada como una herramienta para combatir crímenes como el falso secuestro y el uso de teléfonos celulares por parte de delincuentes desde la prisión. No obstante, más allá de la falta de evidencia del vínculo entre el registro obligatorio y las tasas de criminalidad, se ha visto que el sistema de registro entorpece el acceso de los turistas, quienes requieren registrarse previamente para la obtención de un número de identificación fiscal brasileño antes de poder adquirir una línea telefónica para su estadía (Costa, Casemiro y Pessoa, 2015).

En 2013, ANATEL dictó una medida con la finalidad de denegar el servicio de telefonía móvil a dispositivos falsificados (denominados "xing-ling") a partir de enero de 2014. Para ese momento, se calculaba que estos dispositivos representaban más del 12 % de todo el mercado (Carneiro, 2013), lo que significaba alrededor de 34.5 millones de dispositivos móviles. Sin embargo, la implementación efectiva de esta medida ha resultado cuando menos problemática, al tratarse de un banco de datos gigantesco y complejo. Así, ANATEL ha optado por postergar la medida, que apenas entró en "fase experimental" en 2016.

En este contexto, el Instituto de Tecnología y Sociedad de Río, junto a la organización internacional Access Now, remitieron a ANATEL sus preocupaciones con respecto a las implicancias de esta medida sobre los derechos humanos. Dado que la mayor parte de estos usuarios han adquirido los dispositivos actuando de buena fe, negarles acceso a Internet y a las comunicaciones violenta sus derechos de libertad de expresión y acceso a la información. Aunado a esto, este tipo de medida afecta de manera desproporcionada a los usuarios más empobrecidos, quienes acuden con mayor frecuencia a dispositivos menos costosos, y a quienes les sería especialmente difícil reemplazarlos o adquirir nuevos teléfonos.

5. Perú

5.1. Retención de datos

El Decreto Legislativo Nº 1182 de julio de 2015 (popularmente conocido como Ley Stalker) instauró un mandato obligatorio de retención de datos "derivados de las telecomunicaciones" por tres años. Este mandato pone a disposición de los organismos policiales detalles relativos a las comunicaciones cuya extensión y alcance no está precisada por la normativa, si bien sí establece como requisito la existencia previa de una autorización judicial. No obstante, esta ley ha sido objeto de críticas por la sociedad civil, al haber sido creada directamente por el Poder Ejecutivo a través de un mecanismo excepcional y sin debate previo (Morachimo, 2015). Asimismo, este Decreto Legislativo no deja suficientemente claro qué datos se encuentran comprendidos dentro del concepto genérico de "datos derivados de las telecomunicaciones", una ambigüedad que organizaciones dedicadas a los derechos humanos han evaluado como peligrosa.

Al mismo tiempo, la Ley Nº 27.336 ya establecía una obligación por la cual las entidades bajo la fiscalización del Organismo Supervisor de Inversión Privada en Telecomunicaciones debían conservar los registros fuente y los detalles de facturación de los servicios prestados por un mínimo de tres años.

Aunado a esto, el Código Procesal Penal peruano, en su artículo 230, señala que los prestadores de servicios de telecomunicaciones están obligados a facilitar la información de geolocalización de teléfonos móviles, así como la intervención, grabación o registro de las comunicaciones, de manera inmediata, en tiempo real y de forma ininterrumpida, cuando esta haya sido ordenada a través de una resolución judicial. En cambio, desde la entrada en vigencia del Decreto 1182, la orden judicial deja de ser necesaria, puesto que los órganos policiales pueden requerir a las operadoras acceder a los datos de geolocalización de sus usuarios en tiempo real, sin ningún tipo de autorización previa.

5.2. Registro de teléfonos móviles

Desde el año 2015, las empresas que prestan servicios de telefonía móvil en Perú están obligadas a verificar la identidad de sus usuarios de servicios prepago al momento de la contratación. La obligatoriedad de esta verificación entró en vigencia en enero de 2017, y se lleva a cabo a través de sistemas de identificación biométrica conectados a la base de datos del Registro Nacional de Identificación y Estado Civil. Esta información es centralizada por OSIPTEL en el Registro Nacional de Terminales Móviles, que a su vez contiene la información de todos los usuarios que hayan contratado servicios en cualquier modalidad (OSIPTEL, 2015).

Así, el Reglamento de la Ley Nº 28.774 establece que los proveedores de servicios deberán contar con un Registro Privado de Abonados, en el cual deberá constar el nombre y apellido de cada usuario, junto con su número de identificación (DNI, carnet de extranjería o Registro Único de Contribuyente), el número telefónico y la marca, modelo y serie del dispositivo móvil, incluso cuando el equipo no haya sido comercializado por la empresa en cuestión. Asimismo, el Reglamento obliga a las prestatarias de servicios de telecomunicaciones a implementar un sistema automatizado que les permita registrar si

un usuario utiliza su tarjeta SIM en un dispositivo diferente al registrado. Igualmente, deben entregar a OSIPTEL los registros de los terminales móviles que sean reportados como robados, hurtados, perdidos o recuperados.

Por otra parte, en enero de 2017 se promulgó en Perú el Decreto Legislativo Nº 1338, mediante el cual se crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad (RENTESEG), con la finalidad alegada de "prevenir y combatir el hurto, robo y comercio ilegal de equipos terminales móviles". Este decreto crea un sistema de listas negra y blanca, determinando que solo los equipos incorporados en la lista blanca están habilitados para operar en la red, y que los dispositivos reportados como perdidos, sustraídos o inoperativos estarán inhabilitados. Al activar un equipo móvil, el IMSI y el IMEI quedan así asociados a la identidad específica del usuario autorizado para el uso de ese dispositivo. Con la entrada en vigencia de este decreto, las empresas prestadoras de servicios de telecomunicaciones quedan obligadas a verificar la identidad del usuario al momento de la contratación del servicio, a través del sistema de verificación biométrica de su huella dactilar.

6. Argentina

6.1. Retención de datos

Si bien Argentina no posee un dispositivo legal que consagre con carácter expreso la obligación de retener datos, el Reglamento de calidad de los servicios de telecomunicaciones contempla la obligación por parte de los proveedores de servicio a garantizar cualquier información que las autoridades consideren pertinentes con miras a la realización de evaluaciones de calidad del servicio. Como consecuencia de ello, el artículo 8 de este Reglamento obliga a las compañías de telecomunicaciones a conservar los datos que sus sistemas reciban en el transcurso de la prestación del servicio, por un mínimo de tres años.

Asimismo, la Ley N° 25.873 y su correspondiente decreto reglamentario establecían la obligación de los prestadores de servicio de telecomunicaciones de registrar los datos filiatorios y domiciliarios de sus clientes, así como los registros de tráfico de sus comunicaciones, y sistematizarlos a disposición del Poder Judicial y del Ministerio Público, hasta por un plazo de diez años. Sin embargo, esta norma fue declarada inconstitucional por violar los principios de necesidad, legalidad y proporcionalidad.

6.2. Registro de teléfonos móviles

En noviembre de 2016, a través de la Resolución Conjunta N° 6-E/2016, el Ministerio de Comunicaciones y el Ministerio de Seguridad argentinos crearon el Registro de Identidad de Usuarios del Servicio de Comunicaciones Móviles. Bajo esta normativa, se busca impulsar la nominación de todas las líneas telefónicas existentes en el país, responsabilidad que recae en las operadoras del servicio de telefonía. Dado que, en la práctica, las líneas postpago ya se encuentran asociadas a un titular registrado, el objetivo de esta regulación consiste en generar un registro de las líneas prepago. El primer problema que presenta esta normativa es de orden formal y radica en el hecho de que una disposición de este tenor haya sido dictada por vía administrativa; cabe recordar que uno de los principales requisitos a las restricciones legales a derechos fundamentales es que deben pasar por el proceso ordinario de formación legislativa.

Sumado al registro de líneas telefónicas, ENACOM habilitó en 2016 un sitio web donde los usuarios argentinos pueden consultar la base de datos de GSMA, contentiva de una lista negra internacional de los códigos IMEI de celulares hurtados, robados o extraviados. A los dispositivos cuyos IMEI se encuentren en esa lista negra les será denegado el servicio por parte de las operadoras, de modo que la lista funge como una herramienta mediante la cual un usuario puede saber si determinado dispositivo funcionará en la red móvil antes de adquirirlo (Sametband, 2016). En consecuencia, es evidente que el sistema tiene ciertas limitaciones, pues el usuario precisa tener el dispositivo móvil en la mano, o en todo caso el código IMEI del dispositivo, antes de realizar la transacción.

En este contexto, resulta especialmente preocupante la vaguedad de la resolución 6-E/2016 con respecto a cuáles datos deben ser solicitados a fines del registro, vaguedad que deja esta importante decisión en manos de las operadoras del servicio. Si bien está planteado como un registro de las líneas

telefónicas, y no de los dispositivos, el conjunto formado por ambas normativas ha sido presentado como un solo sistema, y la Ministra de Seguridad declaró que "` [s]i un nuevo chip es conectado a un teléfono en la lista, la línea entonces deberá ser dada de baja". La norma, además, es insuficientemente clara con respecto a las razones que pueden aducir el Ministerio Público o el Poder Judicial para requerir acceso al Registro, así como sobre los términos de dicho acceso (ADC, 2016).

7. México

7.1. Retención de datos

La Ley Federal de Telecomunicaciones y Radiodifusión obliga a las empresas prestadoras de servicios de telecomunicaciones a conservar los metadatos de las comunicaciones de sus usuarios por dos años. Es criterio de la Corte Suprema que las solicitudes de estos datos deben estar precedidas por una orden judicial. El Código Nacional de Procedimientos Penales permite la localización geográfica de los dispositivos de comunicación en tiempo real, si bien establece que la intervención de las comunicaciones y extracción de los datos de identificación de las mismas requerirá orden judicial. Igualmente, el Código establece que los proveedores de servicios estarán obligados a entregar al Ministerio Público, previa orden judicial, los datos conservados respecto a sus usuarios en el ámbito de la prestación del servicio. Este Código no establece ningún tipo de parámetro o límite con respecto a qué datos debe conservar el proveedor del servicio, por cuánto tiempo o bajo qué estándares o criterios.

Por su parte, la Ley Federal de Telecomunicaciones delimita un amplísimo espectro de datos relativos a las comunicaciones que deberán ser conservados por los prestadores de servicio, a fines de entregarlos a las autoridades cuando sean requeridos. Entre estos datos se encuentran:

- el tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos),
- servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);
- datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil:
- número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;
- datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;
- la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;
- la ubicación digital del posicionamiento geográfico de las líneas telefónicas.

7.2. Registro de teléfonos móviles

Entre 2009 y 2011, la Ley Federal de Telecomunicaciones mexicana contempló una política de registro de usuarios de telefonía móvil, a través del Registro Nacional de Usuarios de Telefonía Móvil (RENAUT). Este registro fue creado mediante una resolución de la Comisión Federal de Telecomunicaciones, con la finalidad de responsabilizar a los prestadores de servicio de colaborar con las autoridades en la persecución de delitos cometidos por los usuarios. En la práctica, el RENAUT asociaba a cada usuario de telefonía móvil con su número de identificación nacional (Clave Única de Registro de Población, o CURP). El artículo 44 de la Ley de Telecomunicaciones del 2009 obligaba a los concesionarios de redes públicas de telecomunicaciones a llevar un registro de los datos de sus usuarios (tanto

en prepago como en postpago) que debía incluir, como mínimo, el número de modalidad de la línea telefónica, el nombre completo, domicilio, nacionalidad, número y demás datos de identificación oficial y la impresión de la huella dactilar del usuario. Este mismo artículo establecía que los concesionarios tenían la obligación de conservar las copias fotostáticas o electrónicas de los documentos que sirvieran de soporte a dicho registro.

A pesar de que esta legislación buscaba establecer mecanismos que permitieran mejorar las comunicaciones entre los concesionarios de telecomunicaciones y las autoridades llamadas a combatir el crimen, apenas dos años después de su promulgación fue revertida, tras la admisión por parte de los legisladores de que el RENAUT, no había rendido frutos en la prevención, investigación y persecución de los delitos que buscaba combatir, siendo que en 2010, el primer año de vigencia del registro, la cifra de secuestros se elevó un 8% con respecto a 2009 (Torres Mercado, Castro Trenti, y González Alcocer, 2011). Igualmente, antes de la implementación del registro, se llevaban a cabo alrededor de 4.400 llamadas de extorsión al día, cifra que se incrementó en más del 40%. En el caso mexicano, luego del experimento fallido que significó el RENAUT se comprendió que la pretensión de que un registro de teléfonos móviles disminuya las tasas de criminalidad partía del supuesto -erróneo- de que los criminales utilizarían dispositivos registrados bajo sus propios nombres.

Tal como otros estudios han señalado, el registro de un teléfono móvil a través de un número de identificación único, como el CURP, no garantiza que los datos sean veraces o se mantengan vigentes, máxime cuando no se establecieron incentivos para que las personas mantuvieran sus datos actualizados. En el caso mexicano, por el contrario, la obligación de registrar los dispositivos generó incentivos para el robo de equipos móviles. Estos factores, aunados a la enorme facilidad de defraudar al sistema de registro, creando inconvenientes para usuarios inocentes, llevó al Congreso a la derogación del Registro Nacional de Usuarios de Telefonía Móvil en 2012, apenas dos años después de su entrada en vigencia, determinando que no había contribuido "a la prevención, investigación y/o enjuiciamiento de delitos relacionados". Entre otros argumentos, se señaló que la medida no solo no garantizaba la veracidad de los datos, sino que podía llevar a acusar falsamente a una persona que hubiera sido víctima de robo de identidad. En este sentido, se evaluó que era posible que la política hubiera incentivado actividades delictivas como el robo de teléfonos móviles o la clonación de tarjetas SIM. Junto con la eliminación del RENAUT, los datos recabados a causa de su implementación fueron eliminados, junto con el respaldo de los datos de verificación que contemplaba el mencionado artículo 44.

En la actualidad, México conserva un sistema de lista negra de códigos IMEI; los usuarios pueden reportar un dispositivo como robado o extraviado, y las empresas prestadoras del servicio de telefonía móvil están obligadas a mantener una base de datos y a celebrar convenios que les permitan intercambiar información sobre dispositivos reportados como robados o extraviados, de modo tal que denieguen la activación a dispositivos que muestren códigos IMEI que aparezcan en dicha base de datos (Instituto Federal de Telecomunicaciones, México).

8. Chile

8.1. Retención de datos

En Chile, el estatuto en materia de retención de datos se encuentra disperso entre diversos cuerpos normativos.

De acuerdo con la Ley General de Telecomunicaciones (en su artículo 24H) los prestadores de servicios tienen otras obligaciones, entre las cuales se encuentra proteger la privacidad de sus usuarios y cumplir con deberes generales de confidencialidad. Esta obligación es reiterada por el Reglamento de Servicios de Telecomunicaciones (decreto 18 de 2014), que en su artículo 50 señala que los proveedores de servicios de internet procurarán preservar la privacidad y la seguridad de los usuarios en la utilización de dicho servicio. Se reitera el precepto contemplado en la ley general, no obstante, la amplitud y vaguedad de esta obligación nos obliga a preguntarnos qué debemos interpretar por privacidad y seguridad en el contexto de este marco normativo.

En contraposición al carácter general y difuso de la Ley General de Telecomunicaciones y del Reglamento, la legislación penal ofrece regulaciones más concretas sobre la materia. El ya mencionado artículo 222 establece que el juez de garantía tendrá competencia para ordenar, a petición del Ministerio Público, la interceptación y grabación de las comunicaciones telefónicas o de otra índole de una persona, cuando existan fundadas sospechas, basadas en hechos determinados, de que dicha persona hubiere cometido o participado en la preparación o comisión, o preparare actualmente la comisión o participación en un hecho punible que mereciera pena de crimen.

El Código Procesal Penal (en lo sucesivo, CPP) exige que, en caso de solicitarse la intervención de una comunicación telefónica, se cumplan una serie de requisitos previos para que el Juez de Garantía autorice la medida. Estos requisitos, según puede observarse del texto de la ley, son exhaustivos en comparación con los requisitos de otras medidas contempladas en la misma normativa (por ejemplo, las relativas a la intercepción de correspondencia), generando de este modo una disparidad referente a los tratamientos de la intervención de comunicaciones efectuadas a través de un dispositivo móvil cuando estas son consideradas correspondencia y cuando son consideradas comunicación telefónica. Así, un juez exigirá menos requisitos para intervenir un correo electrónico que para intervenir una llamada, lo que indica que la norma no previó el avance de la tecnología, que conlleva como consecuencia el hecho de que los teléfonos móviles y dispositivos similares hoy en día reúnan más de un mecanismo de comunicación.

Esto se traduce en que las empresas telefónicas quedan obligadas a proporcionar a los funcionarios en cuestión las facilidades necesarias para que tal medida se lleve a cabo en la oportunidad requerida. Para esta finalidad, dichos proveedores deberán mantener un listado actualizado, con carácter reservado y a disposición del Ministerio Público, que contenga sus rangos autorizados de direcciones IP, así como un registro mínimo de un año de los números IP de las conexiones que realicen sus abonados. Es en esta disposición donde salta a la vista el primer fallo grave en la redacción de la norma, ya que esta no señala un límite temporal en cuanto respecta al tiempo máximo por el cual los proveedores pueden almacenar los datos recabados, circunstancia que

rompe con toda proporcionalidad de la medida. La legislación actual chilena en materia de datos personales no establece límites temporales con respecto a la retención de estos, e igualmente omite prescribir parámetros relativos a las condiciones mínimas y estándares de seguridad en torno al almacenamiento de los datos, así como a su eliminación definitiva.

Si bien la redacción del texto legal resulta cuando menos ambigua en lo que respecta a la extensión y alcance de los datos a recabar por los proveedores de servicio, el Ministerio Público, a través del Oficio FN N° 060-14 ("Instrucción general que imparte criterios de actuación aplicables a la etapa de investigación en el proceso penal") confirma que dichas empresas no se limitan a llevar registro de los números IP, sino que igualmente recaban otros metadatos, incluyendo, por ejemplo, los datos relativos al tráfico de las llamadas y los servicios de mensajería:

> Los fiscales, en la solicitud que realicen al respectivo tribunal de garantía, deberán indicar cuál es el alcance de la solicitud de interceptación que están requiriendo, para lo cual señalarán expresamente si solo se solicita la interceptación de la voz o si, además, requieren que el tribunal autorice la obtención del tráfico de llamadas, la información proveniente de los servicios de mensajería u otras formas de telecomunicación que sean posibles de interceptar, conforme a las capacidades técnicas de las operadoras.

El Decreto 142 (Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de telecomunicación) establece los mecanismos de ejecución de la intervención y registro de las comunicaciones, estableciendo que estas deben llevarse a cabo en los términos establecidos por una orden judicial, y que el procedimiento debe respetar la privacidad y seguridad de las comunicaciones que caen fuera del ámbito de la medida. Esta norma establece un plazo mínimo de seis meses para la conservación de los datos de IP de los usuarios; sin embargo, al ser un reglamento, prima el mandato legal contenido en el CPP, donde el plazo mínimo es de un año.

Ninguna de las normativas mencionadas establece un límite temporal de retención de los datos, ni tampoco estándares mínimos en cuanto a su conservación, seguridad y borrado. En general, el consenso respecto a la legislación actual chilena en materia de datos personales es que la protección resulta débil e insuficiente (Viollier, 2017), dado que, más que ofrecer protección a los derechos de las personas, crea un marco regulatorio para el mercado de las bases de datos personales. Al carecer de mecanismos de resguardo y estándares para la conservación de los datos, la legislación vigente permite que sean comercializados, incluso a través de las fronteras, sin consentimiento del usuario. Por otra parte, la ausencia de sanciones efectivas y la inexistencia de una autoridad de control asimismo debilitan la protección que esta ley puede ofrecer.

Al momento de escribir estas líneas, Chile prepara un proyecto de ley de datos personales, proyecto que, además de haber sido esperado y negociado durante largo tiempo, se teme que no pueda llegar a feliz puerto como consecuencia de una agenda pública centrada en el tema electoral (Viollier, 2017b). Este proyecto introduciría diversos cambios a la protección vigente a los datos personales, entre ellos, el derecho a la portabilidad de los datos personales, que permitiría a los ciudadanos requerir una copia de los datos que le conciernen, y crea un procedimiento especial para el ejercicio de los derechos de acceso y rectificación. En este sentido, el proyecto busca una

protección más estricta al requisito de consentimiento previo por parte del titular de los datos, requisito que es tratado de forma más bien laxa por la ley vigente.

Por otra parte, el proyecto reduce el concepto actual de dato personal, excluyendo de dicho carácter a aquellos datos que no son identificables por "medios razonablemente utilizados". Este concepto ambiguo resulta, cuando menos, peligroso, por cuanto abre espacios para el tratamiento abusivo de datos que puedan considerarse que no "califican" para la protección otorgada por la ley.

Por otra parte, la ley vigente no incluye un límite temporal de retención de datos, y el texto actual del proyecto preserva este problema al tiempo que pretende solucionarlo, al establecer que "[l]os datos personales deben ser conservados solo por el período de tiempo que sea necesario para cumplir con los fines del tratamiento". Este parámetro no dista del texto actual, que señala que "[l]os datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado." Estas normas programáticas no respetan el principio de proporcionalidad y constituyen límites insuficientes y difusos, que abren espacios para el abuso por parte de organismos públicos y privados así como de las empresas proveedoras del servicio.

8.2. Registro de teléfonos móviles

En marzo de 2017, Chile implementó una política de pre-registro de códigos IMEI, es decir, un sistema de lista blanca que requiere que los dispositivos móviles aparezcan en el registro antes de ser activados. Hasta el momento, Chile manejaba un registro de lista negra, que permitía a los usuarios reportar los dispositivos cuando éstos fueran robados o hurtados, con la finalidad de que las operadoras móviles pudieran proceder a su bloqueo. La nueva normativa, denominada Ley de Etiquetado de Celulares, exige que los usuarios que adquieran dispositivos móviles fuera del territorio chileno acudan ante una oficina autorizada por la Subsecretaría de Telecomunicaciones de Chile (Subtel), donde se registrará el código IMEI, junto a otros datos como el sistema operativo del dispositivo. Esta última medida entrará en vigencia a partir de julio de 2017. La base de datos, tal como está descrita en la ley, no contempla registrar el nombre del usuario ni otros datos relativos a este, como su domicilio; sin embargo es negligible el esfuerzo necesario para cruzar esa información con la información relativa a la titularidad de la línea telefónica.

En ese sentido, al momento de escribir estas líneas, en Chile se discuten diversos proyectos de ley sobre registro de tarjetas SIM de teléfonos celulares, que pretenden sumarse a la normativa ya existente sobre registro y conservación de datos en el ámbito de las telecomunicaciones y en el ámbito procesal penal.

El primero de estos proyectos de ley (Boletín N° 9767-15) ingresó a la Cámara de Diputados el 9 de diciembre de 2014. En este texto se exige a los operadores de telefonía móvil registrar los datos personales de aquellos clientes que adquieran una línea en la modalidad prepago. Del texto se desprende que su finalidad central radica en disminuir el número de llamados de broma que afectan al número de emergencia de Carabineros de Chile y, en segundo lugar, prevenir actos criminales relacionados con la colocación de artefactos explosivos. Alegan los legisladores que ambas circunstancias podrían ser evitadas en caso de que se tuviera un registro que no permita el anonimato de quienes perpetran

dichos actos, dado que -afirman- esto permitiría perseguir a los culpables de forma más idónea. Vale puntualizar que este texto toma como precedente la ya mencionada Directiva de la Unión Europea, que, como puntualizamos, fue dejada sin efecto por el Tribunal Europeo a causa de sus severos problemas en cuanto a la protección de los derechos humanos.

El texto de este proyecto de ley contiene apenas cinco artículos, que contemplan la obligación de los operadores de telefonía móvil a llevar el registro de tarjetas SIM de los dispositivos prepago a los cuales prestan servicio, un registro que debe contener el nombre y apellido del usuario, su nacionalidad y su número de RUT. Conforme a este proyecto, el registro debería ser remitido a la Subsecretaría de Telecomunicaciones cada seis meses, así como entregados a las autoridades policiales y al Ministerio Público en caso de que lo soliciten, con la finalidad de investigar y enjuiciar hechos constitutivos de delito. Asimismo, se establecen multas de diez a cincuenta unidades tributarias en caso de que las empresas incumplan con estas exigencias. Esta propuesta, extremadamente concisa, omite señalar parámetros para la conservación de estos datos, incluyendo el tiempo máximo de preservación de los mismos. Por otra parte, tampoco establece sanciones asociadas al no cumplimiento de la obligación de registro, a pesar de que en su parte expositiva afirma que se pretende bloquear la SIM en caso de no llevarse a cabo el registro pertinente.

Entretanto, en el Senado reposan dos proyectos de ley sobre registro de dispositivos móviles, referidos a los mismos temas que el proyecto antes mencionado, solo que por separado. En 2014, miembros de la Cámara alta presentaron un proyecto sobre llamadas telefónicas inoficiosas realizadas a servicios de emergencia, y en 2015, inició la discusión de una segunda moción parlamentaria referida a la recolección de datos de usuarios de servicios prepago. En ambos casos se trata de modificaciones a la Ley General de Telecomunicaciones existente.

El primero de estos dos proyectos (el Boletín Nº 9597-07) pretende imponer a los prestadores de servicios de telecomunicaciones la obligación de entregar la información de sus usuarios tanto a Carabineros de Chile como a otros servicios de emergencia, con la finalidad de sancionar el uso indebido de llamadas a estos servicios. En los fundamentos de este proyecto se sostiene que el 80% de las llamadas al servicio de emergencia "133" consisten en comunicaciones oficiosas, bromas y denuncias de sucesos falsos, argumentando que la razón de este fenómeno se encuentra en la falta de sanción ante tales conductas. Este proyecto no plantea la recolección de datos adicionales de los usuarios, sino que deja claro que los datos con los cuales actualmente cuentan las empresas (como la ubicación geográfica según la celda de conexión del dispositivo) son suficientes para individualizar a los usuarios. Así, únicamente contempla que los proveedores deberán facilitar a las autoridades estos datos con relación a los ciudadanos que hagan uso de los servicios de emergencia.

El segundo proyecto (el Boletín Nº 9.894-15) persigue la obligatoriedad de la recolección de datos de usuarios de servicios telefónicos de prepago, con miras a su individualización, es decir, constituye propiamente una normativa de registro obligatorio de dispositivos móviles.

Este proyecto se enfoca en el registro de teléfonos en servicio prepago, enmarcándose así en una tendencia regional y global que apunta a asimilar la flexibilidad de este tipo de servicio (dada la ausencia de un contrato y de ciertas formalidades que el servicio de postpago sí presenta) con el anonimato, y este último con la voluntad y facilidad de delinquir. Así, en los fundamentos de este proyecto se señala

que en Chile existen actualmente más de dieciséis millones de teléfonos en modalidad prepago, equipos que deberán también ser registrados en caso de aprobarse la norma. Sin embargo, el texto afirma que se busca interferir lo menos posible en las características y en la flexibilidad propia del servicio prepago, enfocándose fundamentalmente en la diversidad de locales comerciales donde puede adquirirse una tarjeta SIM.

Así, los datos a solicitarse para la creación de este registro son el nombre completo del usuario, su domicilio, su cédula de identidad o número de pasaporte, así como los datos técnicos del dispositivo y de la tarjeta SIM.

Las diferencia más importante entre estos proyectos radica en la finalidad. En tanto el proyecto relativo a las llamadas inoficiosas busca abordar un problema concreto a través de medidas proporcionales y que no implican la recolección de datos adicionales, el proyecto de la Cámara baja busca lo que en efecto no es sino la eliminación del anonimato en las comunicaciones móviles, una medida que no solo afectaría el libre flujo de información, sino que perjudicaría a los sectores más vulnerables de la población. A pesar de que el proyecto mismo afirme que busca interferir lo menos posible en los esquemas de prestación del servicio, es inevitable que una medida de este tipo afectará su funcionamiento. El registro obligatorio de SIM afecta el mercado de diversas formas, que incluyen una disminución en las tarjetas SIM activas y por ende en el número de usuarios, un alza en los costos de transacción asociados al cambio de compañía telefónica, un aumento de la información disponible en manos de las empresas de telecomunicaciones (que trae como consecuencia la perfilización y mercantilización de esos datos); todos estos costos serán traspasados al usuario final.

9. Conclusiones

Siguiendo los principios anteriormente citados, que deben regir en la aplicación de medidas que restringen el libre tránsito de las comunicaciones, lo primero que debemos señalar es que las medidas de retención de datos a priori no son nunca proporcionadas, por cuanto exigen el manejo de enormes cantidades de información sobre las comunicaciones de todos los usuarios, en general bajo la justificación de perseguir delitos que solo son cometidos por una fracción de ellos. Tal como ha señalado el Consejo de Derechos Humanos de la ONU, las medidas de esta índole no son nunca necesarias ni proporcionales (UNHRC, 2014).

Lo mismo sucede con respecto al registro obligatorio de tarjetas SIM, una práctica que vulnera el derecho de los individuos a expresarse de manera anónima, además de afectar gravemente el acceso a las comunicaciones de una fracción importante de la población. En este sentido David Kaye, Relator especial para la promoción y protección del derecho a la libertad de expresión de Naciones Unidas, ha señalado que medidas como el registro obligatorio de tarjetas SIM:

> socavan directamente el anonimato, en particular para aquellos que acceden a internet solo a través de la tecnología móvil. El registro obligatorio de SIM cards puede proporcionar a los gobiernos la capacidad de monitorear a individuos y periodistas más allá de cualquier interés legítimo del gobierno.[2]

Una segunda preocupación en torno a este tipo de medidas radica en las posibilidades de transmisión e intercambio de estos datos para ser cruzadas o combinadas con otras bases de información. Por ejemplo, en contextos de protesta es posible aplicar simuladores de torres de telefonía móvil y así extraer información de los ciudadanos que se encuentran presentes, que posteriormente puede ser cruzada con las bases de datos de los usuarios para identificarlos sin rastro de dudas. Este riesgo se agrava aún con mayor profundidad en el caso de los países que utilizan tecnologías biométricas.

Por otra parte, como analizábamos al principio de este estudio, siguiendo las categorías de identidad de Gary Marx, los datos que ya reposan en manos de las compañías de telecomunicaciones son más que suficientes en la mayoría de los casos para identificar plenamente a un usuario en caso de ser necesario, sin que haga falta para ello almacenar o recabar una mayor cantidad de información.

Continuando con la aplicación de los principios, encontramos otros conflictos en las legislaciones analizadas. En aquellos países donde las medidas de retención de datos o de registro de tarjetas SIM son tomadas por vía administrativa, el principio de legalidad se ve violentado. Es este el caso de Argentina, cuyo registro obligatorio de SIM fue creado por vía de una resolución ministerial conjunta, y es el caso también de Perú, donde el mandato obligatorio de retener datos de las telecomunicaciones se crea por un Decreto legislativo.

Por último, la existencia de garantías judiciales es un requisito indispensable, en el entendido de que el acceso a estos datos por parte de los órganos investigativos y policiales deberá hacerse caso por caso

2 A/HRC/29/32, párrafo 51

y previa orden judicial. En materia de retención de datos, Perú actualmente permite, en virtud del Decreto 1182, que los órganos policiales requieran a las operadoras acceder a los datos de geolocalización de sus usuarios en tiempo real, sin ningún tipo de autorización previa (Morachimo, 2015). Ahora bien, en materia de registro de tarjetas SIM, es la práctica habitual consagrada en estas normativas que las empresas de telecomunicaciones entreguen estos datos de forma preventiva y periódica a un órgano administrativo, sin que en general se establezca ninguna posibilidad por parte del usuario de ejercer control sobre estos datos.

En este sentido, mal podríamos realizar recomendaciones al Estado chileno en torno a la eventual creación de un registro obligatorio de tarjetas SIM: es nuestra opinión que las eventuales consecuencias negativas de implementar una medida de esta índole contrarrestan por mucho sus posibles ventajas. Sin embargo, en términos generales respecto a las normativas existentes en Latinoamérica, recomendamos a los estados:

- Asegurar que las normativas que busquen regular el acceso a las telecomunicaciones cumplan con el proceso ordinario de formación legislativa.
- Establecer plazos máximos claros y precisos de conservación y registro de comunicaciones, que deben ser breves, teniendo en cuenta la magnitud de la vulneración a los derechos fundamentales que significa esta medida y su proporcionalidad con el fin alcanzado.
- Establecer protocolos de seguridad para el almacenamiento, manejo y comunicación de la información registrada, que contemplen exigencias técnicas precisas, acordes a la sensibilidad de la información de que se trata.
- Establecer sanciones que permitan la aplicación efectiva de dichos estándares a quienes incumplan con estos, así como a quienes vulneren los deberes de confidencialidad o usen estos datos con un fin distinto a aquel con el que fueron registrados.
- Establecer garantías de control judicial previo y obligatorio a través de las cuales el órgano judicial pueda garantizar el cumplimiento de los requisitos de idoneidad, necesidad y proporcionalidad de la medida.

Referencias

ADC (2016): "Preocupaciones acerca del Registro de Identidad de Usuarios de celulares". Consultado en: https://adcdigital.org.ar/2016/11/11/preocupaciones-acerca-del-registro-de-identidad-de-usuarios-de-celulares/https://adcdigital.org.ar/2016/11/11/preocupaciones-acerca-del-registro-de-identidad-de-usuarios-de-celulares/

Antonialli, D., & de Souza Abreu, J. (2016). Vigilancia estatal de las comunicaciones en Brasil y la protección de los derechos fundamentales. InternetLab. Consultado en https://necessaryandproportionate.org/es/country-reports/brazil

Argentina (2016). Ministerio de Comunicaciones y Ministerio de Seguridad: Resolución Conjunta 6 - E/2016. Consultado en: https://www.boletinoficial.gob.ar/#!DetalleNorma/153684/20161110

Aririguzo, M., y Agbaraji, E. (2016), Mobile phone registration for a developing economy: gains and constraints. European Journal of Basic and Applied Sciences, Vol. 3 No. 3, 2016. Consultado en http://www.idpublications.org/wp-content/uploads/2016/05/Full-Paper-MOBILE-PHONE-REGISTRATION-FOR-A-DEVELOPING-ECONOMY-GAINS-AND-CONSTRAINTS.pdf

Article 19 (2011), Kenya: Free expression standards should guide fight against "counterfeit" mobile phones. Consultado en: https://www.article19.org/resources.php/resource/2762/en/kenya:-free-expression-standards-should-guide-fight-against-%E2%80%9Ccounterfeit%E2%80%9D-mobile-phones

Assembleia Legislativa do Estado de Sao Paulo: Lei N° 16.269, de 05 de julho de 2016. Consultado en: http://www.al.sp.gov.br/repositorio/legislacao/lei/2016/lei-16269-05.07.2016.html

Brasil (2007). Resolução nº 477, de 7 de agosto de 2007 – ANATEL- Aprova o Regulamento do Serviço Móvel Pessoal – SMP. Consultado en: http://www.procon.go.gov.br/legislacao/resolucoes/resolucao-no-477-de-7-de-agosto-de-2007-anatel-aprova-o-regulamento-do-servico-movel-pessoal-smp.html

Carneiro, Flávio (2013). Celulares piratas serão bloqueados pelas operadoras; aprenda a identificar esses aparelhos. UOL Noticias. Consultado en: https://tecnologia.uol.com.br/noticias/redacao/2013/04/17/detalhes-desmascaram-copias-piratas-de-smartphones-veja-dicas-para-evitar-compra.htm

Chebusiri, W. (2012), Kenya's battle to switch off fake phones, BBC. Consultado en: http://www.bbc.com/news/world-africa-19819965

Chile (2014). Cámara de Diputados. Boletín Nº 9767-15. pp. 1-2. http://www.senado.cl/

appsenado/templates/tramitacion/index.php?boletin_ini=9597-07

Chile (2014). Senado. Boletín N° 9.597-07.En línea, disponible en: http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=9597-07 [Fecha de consulta: 18 de abril de 2016], p.1.

Chile, Subsecretaría de Telecomunicaciones (2016), A partir de marzo se implementará normativa que reducirá el robo de celulares. Consultado en: http://www.subtel.gob.cl/a-partir-de-marzo-se-implementara-normativa-que-reducira-el-robo-de-celulares/

Chile (2016), Ley de Etiquetado de Celulares: Resolución número 1.463 exenta, de 2016.- Fija norma técnica que regula las especificaciones técnicas mínimas que deberán cumplir los equipos terminales utilizados en las redes móviles. Consultado en: http://www.diariooficial.interior.gob.cl/media/2016/06/16/do-20160616.pdf

Chile (2017). Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Consultado en: https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07

Costa, D.; Casemiro, L. y Pessoa, T. (2015): "Telefonia móvel vira corrida de obstáculos para estrangeiros". O Globo, 25 de octubre de 2015. Consultado en: https://oglobo.globo.com/economia/defesa-do-consumidor/telefonia-movel-vira-corrida-de-obstaculos-para-estrangeiros-17870170#ixzz4gxeVFhUShttps://necessaryandproportionate.org/es/country-reports/brazil

Donovan, K., & Martin, A. (2014), The rise of African SIM registration: The emerging dynamics of regulatory change. First Monday, 19(2). doi:http://dx.doi.org/10.5210/fm.v19i2.4351

Eagle News (2016, August 2), SIM card registration to counter prank calls on emergency hotlines. Eagle News. Consultado en http://www.eaglenews.ph/featured-news/sim-card-registration-to-counter-prank-calls-on-emergency-hotlines/

El Mercurio (2014), Supertel y Senae empiezan registro de aparatos celulares. Consultado en: http://www.elmercurio.com.ec/422020-supertel-y-senae-empiezan-registro-de-aparatos-celulares/http://www.eaglenews.ph/featured-news/sim-card-registration-to-counter-prank-calls-on-emergency-hotlines/

Ferrari, V., & Schnidrig, D. (2016). Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina. Consultado en https://necessaryandproportionate.org/es/country-reports/argentina

Flores, P.(2015), Senado de Paraguay rechaza definitivamente la ley #Pyrawebs. FayerWayer. Consultado en: https://www.fayerwayer.com/2015/06/senado-de-paraguay-rechaza-definitivamente-la-ley-pyrawebs/

Fundación Karisma (2016), ¿Es legítima la retención de datos en Colombia? Consultado en: https://karisma.org.co/descargar/es-legitima-la-retencion-de-datos-en-colombia-2/

García, L. F. (2016). Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México. Red en Defensa de los Derechos Digitales. Consultado en https://necessaryandproportionate.org/es/country-reports/mexico

Gow, G. A., & Parisi, J. (2008). Pursuing the Anonymous User: Privacy Rights and Mandatory Registration of Prepaid Mobile Phones. Bulletin of Science, Technology & Society, Vol. 28(1), 60–68.

GSMA. (2013, November). The Mandatory Registration of Prepaid SIM Card Users: A White Paper. Consultado en http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf

GSMA (2016), Mandatory 'real name' registration by prepaid SIM card users: Considerations for policymakers. Consultado en: http://www.gsma.com/newsroom/blog/mandatory-real-name-registration-prepaid-sim-card-users-considerations-policymakers/

GSMA (2017), "Coloured lists. Managed services". Consultado en: http://www.gsma.com/managedservices/mobile-equipment-identity/the-imei-database/coloured-lists/

Guatemala (2013), Decreto Número 8-2013, Ley de Equipos Terminales Móviles. Consultado en: http://ww2.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs%20leyes/2013/pdfs/decretos/D08-2013.pdf

Instituto de Tecnologia & Sociedade do Rio y Access Now (2015). Connectivity at Risk/Study on the impact of blocking uncertified mobile devices in Brazil. Consultado en: https://www.accessnow.org/cms/assets/uploads/archive/docs/ITS_Report_English_Final_1.pdfhttp://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf

Jentzsch, N. (2012), Implications of Mandatory Registration of Mobile Phone Users in Africa (Discussion papers No. 1192). Berlin: Deutsches Institut für Wirtschaftsforschung.

Kapellmann, D., & Reyes, B. (2015). Retención y Privacidad de Datos: Algunas Lecciones Derivadas de las Diversas Prácticas Internacionales. The Social Intelligence Unit, the-siu.net. p. 9. Consultado en the-siu.net

Kaye, D. (2015). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. United Nations, Human Rights Council. Consultado en www.ohchr.org/EN/HRBodies/HRC/.../A.HRC.29.32_AEV.doc

Keane, B. (2015, March 18). Your guide to the data retention debate: what it is and why it's

bad. Crikey. Consultado en https://www.crikey.com.au/2015/03/18/your-guide-to-the-data-retention-debate-what-it-is-and-why-it%E2%80%99s-bad/

México, Instituto Federal de Telecomunicaciones (s/f), ¿Te robaron o perdiste tu celular? Consultado en: http://www.ift.org.mx/usuarios-telefonia-movil/te-robaron-o-perdiste-tu-celular

México (2009), Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones. Consultado en http://dof.gob.mx/nota_detalle.php?codigo=5079751&fecha=09/02/2009https://www.crikey.com.au/2015/03/18/your-guide-to-the-data-retention-debate-what-it-is-and-why-it%E2%80%99s-bad/

Morachimo, M. (2015): Nueva norma permite a la Policía saber dónde está cualquier persona sin orden judicial. Hiperderecho, 27 de julio de 2015. Consultado en: http://www.hiperderecho.org/2015/07/norma-policia-geolocalizacion-sin-orden-judicial-1182/

Morachimo, M. (2016). Vigilancia Estatal de las Comunicaciones y Derechos Fundamentales en Perú. Consultado en https://necessaryandproportionate.org/es/country-reports/peru

OHCHR (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. A/HRC/23/40. Consultado en: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

OSIPTEL (2015): "Desde hoy las líneas móviles prepago se venderán con identificación dactilar de los usuarios". Consultado en: https://www.osiptel.gob.pe/noticia/desde-hoy-lineas-prepago-identificacion-dactilar

Perú (2015). Ley N° 28.774, que crea el Registro Nacional de Terminales de Telefonía Celular, establece prohibiciones y sanciones. Consultado en: http://transparencia.mtc.gob.pe/idm_docs/normas_legales/1_0_3622.pdf

Perú (2017), Decreto Legislativo 1338 que crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad, orientado a la prevención y combate del comercio ilegal de equipos terminales móviles y al fortalecimiento de la seguridad ciudadana. Consultado en: http://busquedas.elperuano.com.pe/normaslegales/decreto-legislativo-que-crea-el-registro-nacional-de-equipos-decreto-legislativo-n-1338-1471014-4/https://necessaryandproportionate.org/es/country-reports/peru

Privacy International. (2004). Mistaken Identity; Exploring the Relationship Between National Identity Cards & the Prevention of Terrorism (Interim report). Privacy International. Consultado en https://web.archive.org/web/20061209185839/http://www.privacyinternational.org/issues/idcard/uk/id-terrorism.pdf

Privacy International, Access, & Electronic Frontier Foundation. (2014, May). Necesarios & Proporcionados. Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Consultado en https://necessaryandproportionate.org/es/necesarios-proporcionados

Privacy International (2017). State of Privacy: Colombia. Consultado en: https://www.privacyinternational.org/node/977

Rodríguez, K. (2014). La Retención de Datos de Tráfico en Paraguay Es Espionaje Masivo e Inconstitucional. Electronic Frontier Foundation. Consultado en: https://www.eff.org/es/deeplinks/2014/11/la-retencion-de-datos-de-trafico-en-paraguay-es-espionaje-masivo-e

Sáenz, P. (2016), Señores Ministerio TIC: ¿Ya intentaron homologar un celular? Yo sí y ¡no pude! Fundación Karisma. Consultado en: https://karisma.org.co/senores-ministerio-tic-ya-intentaron-homologar-un-celular-yo-si-y-no-pude/

Sametband, R. (2016), Habilitan el sitio Web nacional para verificar si un celular es robado. La Nación. Consultado en: www.lanacion.com.ar/1896940-habilitan-el-sitio-web-para-verificar-si-un-celular-es-robadohttps://necessaryandproportionate.org/es/necesarios-proporcionados

Torres Mercado, T., Castro Trenti, F., & González Alcocer, A (2011). Iniciativa con proyecto de decreto por el que se reforman, adicionan y derogan diversas disposiciones del Código Federal de Procedimientos Penales, del Código Penal Federal, de la Ley Federal de Telecomunicaciones y de la Ley que establece las normas mínimas sobre readaptación social de sentenciados, Pub. L. No. Gaceta LXI/2SPO-228/28925.

Tribunal de Justicia de la Unión Europea. (2014 8). Comunicado de prensa N. 54/14. Consultado en http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf

United Nations Human Rights Council. (2014), The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights. United Nations Human Rights Council. Consultado en http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc

Viollier, P. (2017), El estado de la protección de datos personales en Chile. ONG Derechos Digitales. Consultado en: https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf

Viollier, P. (2017b), Protección de datos: una buena noticia a medias, en un Chile a medias. ONG Derechos Digitales. Consultado en: https://www.derechosdigitales.org/11003/proteccion-de-datos-una-buena-noticia-a-medias-en-un-chile-a-medias/http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc

Wallace, K. A. (1999), Anonymity. Ethics and Information Technology, 1, 23–35.


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina