DERECHOS DIGITALES
América Latina

2010-2020

Sucesos regulatorios en materias de **privacidad e internet** *en Latinoamérica*

VALENTINA HERNÁNDEZ B.

Texto por Valentina Hernández Bauzá
Portada y diagramación: Constanza Figueroa.
Edición: Vladimir Garay.

Diciembre de 2020

Contenidos

Resumen ejecutivo

En el presente reporte se analiza la evolución en una década de las tendencias normativas y jurisprudenciales en los países de hispano América y Brasil, en cinco áreas relacionadas a la privacidad, su protección y vulneración a través de medios tecnológicos (protección de datos personales, actividades de vigilancia e inteligencia, delitos contra la intimidad, reglas sobre retención de datos -especialmente en telecomunicaciones- y normas sobre biometría) y los desafíos que tiene la región para enfrentarlos de mejor manera dentro del mediano y largo plazo. Para esto, se utilizaron una serie de bases de datos relevantes en estas materias, así como la búsqueda de legislación y jurisprudencia de manera directa en los portales de los poderes judiciales y legislativos de cada país, y la búsqueda abierta a través de internet.

En particular, sobre datos personales se revisa la legislación dictada en esta década sobre la materia, la recepción de los derechos ARCO, el aumento en el reconocimiento constitucional del derecho a la protección de datos personales, la transferencia transfronteriza y jurisprudencia sobre derecho al olvido. Respecto de actividades e inteligencia, se revisan las medidas de interceptación de comunicaciones, la grabación de estas y la intervención de sistemas informáticos, que han sufrido escasas modificaciones, presumiéndose a menudo la aplicación de reglas de investigación preexistentes a internet. Luego, se tratará el arista de resguardo ante medidas de vigilancia, tales como los requisitos de estas medidas y el reconocimiento de técnicas de cifrado.

En el capítulo de delitos contra la intimidad se señala la cantidad de normativa por países de esta década, la regulación del delito de difusión o revelación de imágenes y material íntimo, la difusión de material íntimo no consentido y el acceso no autorizado a datos, donde las tendencias reflejan avances legislativos como consecuencia de la actualización de las reglas de datos personales y de las normas penales para ajustarlas a la delincuencia cibernética y a los delitos cometidos a través de la red. Sobre retención de datos y registro de identidad de teléfonos se revisan las modificaciones sobre registro de servicios de prepago y tarjetas SIM, además de las medidas de registro de comunicaciones telefónicas y/o digitales, donde existe una tendencia limitada por instaurar nuevos regímenes de registro.

Sobre delitos contra la identidad, existe una moderna tendencia —ya reflejada en Argentina y México— de penalizar los casos de difusión no consentida de material íntimo. Existen además múltiples leyes de inteligencia y combate de delitos que contemplan hipótesis de intervención de comunicaciones y sistemas informáticos, y retención de datos. Cierra este trabajo con biometría, donde se señalará la legislación de la década en estudio y regulación sobre huellas dactilares y ADN, área en que creemos habrá importantes nuevos desarrollos en la década que comienza.

Introducción

La Asamblea General de Naciones Unidas (2016) ha observado que el rápido ritmo del desarrollo tecnológico permite incrementar la capacidad de los gobiernos, las empresas y las personas de llevar a cabo actividades de vigilancia, interceptación y recopilación de datos, lo que podría constituir una violación o una transgresión de los derechos humanos, en particular del derecho a la privacidad, establecido en el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, y que, por lo tanto, esta cuestión suscita cada vez más preocupación:

"…las violaciones y las transgresiones del derecho a la privacidad en la era digital pueden afectar a todos los individuos, incluidas, con repercusiones particulares, las mujeres, así como los niños y quienes son vulnerables o están marginados".[1]

Las revelaciones de Edward Snowden en 2013 dejaron de manifiesto el riesgo sobre la privacidad que significa para la privacidad personal el uso de las herramientas de comunicación. Ya no solamente por la eventualidad de intrusiones delictuales, sino también por el interés político en el registro de comunicaciones por parte de los estados, incluso con la cooperación (voluntaria o no) de empresas privadas que intermedian esas comunicaciones. En 2015, CCCBLab hizo una reseña sobre la vigilancia en América Latina, determinando que diversos gobiernos de la región encargan su propia vigilancia.[2] A esto se suman otras formas de registro de información por parte de los estados y las empresas, como la creciente acumulación de información biométrica, y el uso de tecnologías de vigilancia en espacios públicos.

Estos puntos serán estudiados a continuación, como ejes en los cuales la intervención tanto estatal como privada permiten generar perfiles altamente precisos de cada sujeto. Lamentablemente, la protección normativa no siempre está a la par del avance tecnológico; Cuánto de ello se basa en reglas existentes y formuladas de manera previa a la revolución digital, y cuánto de ello motiva o se basa en modificaciones a la legislación en la última década, es parte de esta breve revisión. De este modo, resaltaremos las tendencias regionales como también los desafíos a futuro para otorgar mayor protección a los individuos ante el desarrollo tecnológico.

1 Asamblea General de las Naciones Unidas. 2016. El Derecho a la Privacidad en la Era Digital. Disponible en: https://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1&referer=/english/&Lang=S

2 CCBLab. 2015. Vigilancia Masiva en América Latina. 2015. Disponible en: http://lab.cccb.org/es/vigilancia-masiva-en-america-latina/

Temáticas en estudio

Protección de datos personales

Legislación

Varios países de la región hicieron modificaciones a sus regímenes de datos personales, mediante la primera introducción de leyes en la materia o por el reemplazo de las reglas antes existentes.

En México, poco antes del inicio de la década, la Constitución federal fue modificada, incorporando en su artículo 16 la protección autónoma de datos personales. En 2010 se integraron a la ley disposiciones expresas para el tratamiento de datos personales en el sector privado, a través de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010), a la que sucedió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017).

En Costa Rica, la Ley Nº 8.968 sobre protección de la persona frente al tratamiento de sus datos personales (2011) es el cuerpo normativo central en la materia, complementada por el Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, Decreto Ejecutivo Nº 37554-JP (2013).

El Salvador no cuenta con una ley general sobre protección de los datos personales, pero a comienzos de la década se dictó la Ley de Regulación de los Servicios de Información sobre el Historial de Crédito de las Personas (2011). Actualmente existe un proceso de estudio de proyecto sobre una ley de protección de datos personales y habeas data. En este estudio se han levantado temas tales como la regulación de aplicaciones que requieren reconocimiento facial, así como aquellas que tienen acceso a la información de teléfonos móviles.[3]

En Colombia existe una ley general, que data de inicios de la década: Ley Estatutaria Nº 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Esta ley sucedió a otras reglas anteriores, como la Ley Estatutaria 1266 de 2008, que regulaba el habeas data y el uso de información en el ámbito financiero y crediticio.

Perú cuenta con la Ley Nº 29.773 de datos personales (2011) como norma principal y su reglamento, el Decreto Supremo Nº 003-2013-JUS (2013).

---

3 Asamblea Legislativa de la República de El Salvador, 05 de junio de 2019, disponible en: https://www.asamblea.gob.sv/node/9644

También Nicaragua creó normativa a principios de la década, mediante la Ley Nº 787 de Protección de Datos Personales (2012) y su reglamento, el Decreto 36/2012, que discurre sobre los tipos de consentimiento y recoge expresamente los derechos de acceso, rectificación, cancelación y oposición. Como curiosidad, en la ley nicaragüense se define el "derecho al olvido digital" en los siguientes términos: "El titular de los datos tiene derecho a solicitar a las redes sociales, navegadores y servidores que se supriman y cancelen los datos personales que se encuentren en sus ficheros".

Más recientemente, entró en vigencia la Ley General de Protección de Datos Personales de Brasil (2018), una de las leyes más modernas en la materia y que ordena la creación de una autoridad pública de control independiente. Poco después, Panamá promulgó su primera ley general en la materia, la Ley Nº 8 de protección de datos personales (2019).

Otros países actualizaron su normativa de datos personales mediante cambios constitucionales. Mediante la Ley Nº 21.096 de 2018, la Constitución Política de la República de Chile incorporó la protección de datos personales dentro de su catálogo de derechos fundamentales.

La Constitución de República Dominicana de 2015 reconoce el derecho de toda persona a decidir sobre la utilización de los datos sobre ella y sus bienes, dentro del artículo correspondiente al derecho a la intimidad y honor personal, e instauran la acción de habeas data dentro del capítulo de las garantías constitucionales. Este país ya contaba con una ley de protección de datos personales, la ley Nº 172-13 (2013).

Si bien Cuba no cuenta con una ley sobre protección de datos personales, la Constitución cubana de 2019 reconoce, en su artículo 97, el derecho de toda persona a acceder a sus datos personales en registros, archivos u otras bases de datos e información de carácter público, así como a solicitar su no divulgación y obtener su debida corrección, rectificación, modificación, actualización o cancelación. Dispone además que el uso y tratamiento de estos datos se realiza de conformidad con lo establecido en la ley.

Otros países aún no cuentan con leyes de aplicación general en materia de datos personales, pero existen avances legislativos en la materia. Es el caso de Ecuador, cuya constitución reconoce la protección de datos personales como un derecho fundamental y regula el habeas data, y que en 2019 hizo público un proyecto de ley orgánica de protección de datos personales.[4]

Paraguay tampoco tiene una ley general de protección de datos personales, pero la Ley Nº 1682 de 2001, que reglamenta la información de carácter privado, contiene varias normas y principios al respecto. Durante la última década, la ley sufrió numerosas modificaciones, principalmente en materias como la actualización de datos patrimoniales, el derecho de toda

4 Ecuador. 2019. Asamblea Nacional. Memorando PAN-CLC-2019-. Proyecto de ley de protección de datos personales. Disponible en el siguiente link: https://www.nmslaw.com.ec/wp-content/uploads/2019/09/Proyecto-de-Ley-Org%C3%A1nica-de-Protecci%C3%B3n-de-Datos-Personales.pdf

persona a recolectar, almacenar y tratar datos y los casos en que los datos patrimoniales y financieros de las personas pueden ser difundidos. Existe además un proyecto de ley de protección de datos personales, presentado en 2019.[5]

Como síntesis de todo lo anterior, podemos decir que en América Latina se ha seguido la tendencia global, estableciendo legislación de protección de datos personales. La tendencia regional apunta a contar con leyes generales destinadas a esta materia, incluso en países donde ya existían normas especiales para ámbitos como el financiero y crediticio.

Como consecuencia de lo anterior, al final de la década nos encontramos con que solo seis países latinoamericanos carecen de una ley de datos personales. Estos son Bolivia, Cuba, Venezuela, Honduras, Ecuador y Guatemala, aunque en todos ellos existe reconocimiento constitucional de alguna clase a la protección de datos personales. En Ecuador ya existe un proyecto de ley y en Guatemala está tomando lugar una serie de discusiones y reuniones destinadas a dicho fin. Paraguay y El Salvador tienen leyes especiales que contienen disposiciones sobre datos personales; para estos efectos se considerarán como leyes especiales de datos personales.

13 de 19 países cuentan con cuerpos normativos (dos con cuerpos no exclusivos) y, de los seis restantes, dos están en proceso de crearlo. Se hace necesario destacar también los casos chileno y argentino. En el primero, actualmente se discute un proyecto de ley de datos personales, buscando reemplazar la normativa existente, que tiene más de veinte años de antigüedad. En Argentina existe un proyecto de ley del año 2018, que busca modernizar la legislación actual.

Hay que mencionar que si bien la tendencia ha sido a legislar, no todos estos países cuentan con una ley global de datos personales, sino una referida a una sección en particular. De 13 leyes dedicadas a la protección de datos personales, 11 de ellas son leyes generales. Las restantes aplican a un ámbito de la protección de datos personales. Así, El Salvador tiene la "Ley de regulación de los servicios de información sobre el historial de crédito de las personas" y Paraguay la "Ley Nº 1682 de 2015 que reglamenta la información de carácter privado". Podemos observar que la tendencia en la región es a contar con una ley global de protección de datos personales.

La década entre 2010 y 2020 además fue fecunda en la dictación de nuevas leyes de datos personales, sin perjuicio de la actualización de las pocas leyes anteriores a este período. Las leyes que datan de una fecha previa al periodo de estudio del presente trabajo son las de Chile (1999), Argentina (2000) y Uruguay (2008), con proyectos de actualización en tramitación (Chile 2017 y Argentina 2018).

En cuanto a su contenido, se observa –superficialmente– que el derecho español constituye

5 Paraguay. 2019. Proyecto de ley de protección de datos personales. Disponible en el siguiente link: https://observatoriolegislativocele.com/paraguay-proyecto-de-ley-de-proteccion-de-datos-personales-2019/

una influencia en la legislación de protección de datos personales regional y en los proyectos de ley que se discuten actualmente. En particular, consideraremos para este punto la incorporación de los derechos ARCO (acceso, rectificación, cancelación y oposición) formulados así, dentro del articulado de la ley de datos de cada país de la región. Al norte de la región, las leyes especiales los recogen de manera expresa en un 62 % de los casos, en México, Nicaragua, Panamá y República Dominicana, además de Perú más al sur. Los proyectos de ley ecuatoriano, argentino y chileno también los incorporan de forma explícita. Así, de ocho legislaciones dictadas o modificadas entre 2010-2020, cinco recogen los derechos arco en su totalidad y dos parcialmente. Luego, tres proyectos de ley de países que actualmente no los contemplan, los incorporan.

Durante esta última década, los países de América Latina han buscado ser centros de desarrollo tecnológico. Para ello, la actualización normativa ha requerido hacerse cargo de un tratamiento de datos personales que no se restringe a las fronteras nacionales, incluyendo aquí la presión por cumplir con los estándares internacionales de protección de datos personales, especialmente europeos, para desarrollar actividades comerciales y lograr que grandes empresas instalen sus oficinas con confianza. República Dominicana, Colombia, Perú, Panamá, Nicaragua, México y Brasil regularon o modificaron la normativa vigente sobre transferencia internacional de datos entre 2010 y 2020, mientras que Argentina, Paraguay, Ecuador y Chile la consideran dentro de sus proyectos de ley.

Jurisprudencia

Algunos casos son ejemplares en materia de protección de datos, en particular en relación con la desindexación de contenidos, como también con la búsqueda de eliminación de artículos de prensa que incluyen información personal como el nombre.

Si bien se trata de una cuestión íntimamente vinculada a la libertad de expresión, en las próximas líneas daremos cuenta de algunas decisiones ejemplares, que dan cuenta de múltiples discusiones en torno a conceptos distintos de "derecho al olvido".

En Chile, la causa fallada por la Corte Suprema en julio de 2019, Rol Nº 1279-2019, estableció que la información de medios de comunicación es de interés público y que no puede ser eliminada, aun tratándose de información personal. Se dictaminó que, no obstante, debe ser actualizada a fin de representar el estado actual de una persona que ya cumplió su condena. Si bien la parte actora argumentó en base al derecho al olvido, tanto la Corte de Apelaciones como la Corte Suprema no dictaminaron en base a este, sino que el máximo tribunal decidió que las versiones digitales de los periódicos involucrados rectificaran la información en vez de retirarla de internet. Si bien el cirujano que dedujo recurso de protección argüía en base al derecho al olvido, este no fue reconocido por el Estado chileno.

En México, en el caso *Anónimo contra Google México*, el Instituto Federal de Acceso a la Información y Protección de Datos ordenó a la empresa *a desindexar ciertas URLs de su motor de búsqueda y borrar información de una persona de sus bases, fundada en la petición de un individuo que señaló que, al buscar su nombre en Google, se revelaba información como su nombre, el de su fallecido padre, el de sus hermanos e información sobre su actividad de negocios. Se determinó que, al hacer pública la información de una persona, esto era tratamiento de datos personales. Se encontró responsable a Google México no obstante que el tratamiento lo realizó Google en Estados Unidos.*

Argentina también tuvo involucrados a los motores de búsqueda Yahoo! y Google, en el caso *Rodríguez vs Google inc*. fallado en 2014. En este, la demandante alegó que se asociaba a resultados a páginas con contenido pornográfico. La máxima Corte de ese país falló que las compañías de buscadores no tienen responsabilidad objetiva, sino un régimen de responsabilidad subjetiva. Así, "se configura en caso de que tengan efectivo conocimiento de la licitud del contenido que se les reprocha y, a pesar de eso, no actúan diligentemente removiendo el correspondiente link".[6] Luego, la Corte Suprema al referirse al contenido mismo decidió que el monitoreo y filtro del contenido podía suponer censura previa.

En Colombia también existe jurisprudencia relevante. La Corte Constitucional conoció en 2013 del caso *Martínez vs Google*, referido a la petición de eliminación de su nombre en información que lo conectaba a un cartel de crimen organizado. Se pidió que se eliminara tanto del periódico que la publicó como del buscador Google. La Corte Constitucional falló que el periódico debía rectificar la información, pero liberó a Google de toda responsabilidad, debido a su rol solamente como intermediario.

En Perú destaca el caso resuelto por la Dirección General de Protección de Datos Personales, Nº 045-2015-JUS/DGPDP. En este, la Dirección determinó que la filial peruana de Google Inc. está sujeta a la ley de protección de datos personales de dicho país, ante un caso en que un sujeto, cuya responsabilidad penal se desestimó, solicitó ser sacado de su motor de búsquedas. Ello, dado que Google busca información que contiene datos personales de ciudadanos peruanos con el fin de facilitar el acceso a la información de sus usuarios, y porque tiene una función de geolocalización que ofrece a los usuarios la opción de solamente recibir información extraída de sitios peruanos.

En Brasil, en el año 2018, en el caso *DPN vs. Google Brasil Internet Ltda*, DPN solicitó a Google, Microsoft y Yahoo! que se removieran de los resultados de búsqueda enlaces con información referente a un caso de fraude. La Corte Superior de Justicia falló a favor de DPN, ordenando a los buscadores sacar de su motor de búsqueda la información que permitiese

---

6 Llorente y Cuenca. 2015. El fallo "Rodríguez vs. Google" de la Corte Suprema de Argentina: ¿hacia una vía latinoamericana para el Derecho al Olvido? Disponible en: https://ideas.llorenteycuenca.com/wp-content/uploads/sites/5/2015/01/150129_informe_especial_reputacion_internet_ESP.pdf

vincular a DPN con el caso de fraude, refiriéndose al “derecho al olvido”.

Los casos colombiano, peruano, brasileño y argentino tuvieron a motores buscadores como partes involucradas. En Perú, se sentenció que su normativa aplicaba a Google (tanto su filial como a la central norteamericana), en tanto el motor trata datos de ciudadanos peruanos y que su función de geolocalización hace que los ciudadanos de dicho país accedan preferencialmente a información originada en Perú. En Brasil se ordenó la desindexación y se reconoció al derecho al olvido de forma expresa. En Colombia, a diferencia de Perú, se liberó a Google de responsabilidad, dado que actúa como intermediario. En Argentina se estableció que los motores de búsqueda no tienen responsabilidad objetiva por el contenido, además, se desestimó la demanda en tanto podría suponer un caso de censura previa.

Actividades de vigilancia y de inteligencia

Existen múltiples actualizaciones legales en materias de vigilancia, tanto para fines de investigación criminal como dentro de actividades de inteligencia. En general, apuntan a generar marcos normativos para la obtención de información útil para los estados, a partir de las formas más modernas de comunicación.

Respecto de la interceptación de comunicaciones, El Salvador cuenta con la Ley Especial para la Intervención de Telecomunicaciones (2010), mientras que en Honduras encontramos el Decreto 243-2011, Ley especial sobre intervenciones de las comunicaciones privadas (2012). En Colombia, la normativa relevante se encuentra en el Código de Procedimiento Penal, específicamente en una modificación realizada en 2011.

Nicaragua cuenta con la Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la administración de los bienes incautados, decomisados y abandonados (2010). Además, es relevante mencionar el Código Procesal Penal de 2014.

En México, si bien existe una ley de seguridad nacional de 2005 que menciona las intervenciones de comunicaciones, es preciso centrar nuestra atención en la normativa del periodo en estudio: la Ley Federal contra la delincuencia organizada (2016) y el Código de Procedimientos Penales (2014).

Normas procesales completas también fueron dictadas durante la década. Es relevante mencionar en el Código Procesal Penal (2019) en Argentina, y el Código Orgánico Integral Penal (2014) en Ecuador, mientras Venezuela cuenta con el Código Procesal Penal (2012). También hubo reforma en Brasil, en una modificación del Código de Proceso Penal del año 2019, referente a los jueces de garantía (Decreto-Lei Nº 3.189. Código de Processo Penal).

También hubo actualizaciones en materia de inteligencia. En Paraguay se dictó la Ley 5241 que Crea el sistema nacional de inteligencia (2014). En tanto Uruguay lo legisló a través de la Ley 29.696, "Aprobación y regulación del sistema nacional de inteligencia del Estado" (2018).

En estas modificaciones se identifican distintas tendencias. En la mayoría de los países de la región existe normativa sobre interceptaciones telefónicas, grabación de comunicaciones e intervención de sistemas informáticos, y la mayoría data de esta década. Sobre el cuerpo normativo que regula estos temas, algunos países lo hacen mediante leyes de inteligencia, otros en Códigos Procesales Penales de carácter general, y otros en leyes de crimen organizado o en normativas especiales sobre interceptación de comunicaciones. En primer lugar, se identifican los países que contienen regulación dictada entre 2010-2020 al respecto: México, El Salvador, Honduras, Nicaragua, Colombia, Ecuador, Paraguay, Uruguay, Venezuela, Argentina y Brasil.

La interceptación de comunicaciones es la medida con mayor presencia a lo largo de la normativa de los países estudiados. Si bien es contemplada en las leyes especiales de inteligen-

cia y crimen organizado como medida investigativa de los delitos o conductas contenidas en tales normas, igualmente se encuentra cubierta en leyes procedimentales penales o en cuerpos normativos completamente dedicados a la medida propiamente tal. Es decir, se regula variablemente a propósito de los delitos investigados como en razón de las medidas investigativas. Es la medida investigativa de mayor data y va de la mano de la grabación de las comunicaciones en los códigos procedimentales, en tanto las comunicaciones no solo se intervienen, sino que también se registran para la posterior escucha de quienes la solicitan a la autoridad judicial. No obstante, hay leyes de inteligencia en que la grabación se considera un procedimiento especial aparte de la interceptación.

De las leyes estudiadas, una de las características presentes es la completa variabilidad de la extensión de las reglas sobre interceptación a distintos tipos de comunicaciones. Esto es, si bien se consideran incluidas usualmente las comunicaciones telefónicas y de correspondencia escrita, es muy variable si las mismas regulaciones alcanzan a los distintos tipos de comunicaciones electrónicas. Una serie de ejemplos así lo demuestra.

El artículo 143 del Código Procesal Penal argentino de 2019 se refiere a la interceptación. Así, dispone que el juez podrá ordenar la interceptación y secuestro de correspondencia postal, telegráfica, electrónica o cualquier forma de comunicación o de otro efecto remitido por el imputado o destinado a este. Aquella tiene el carácter de excepcional. El artículo 146 complementa esta disposición e indica que las intervenciones serán registradas mediante su grabación magnetofónica u otros medios.

El artículo 476 del Código Orgánico Integral Penal de 2014 de Ecuador trata la interceptación de las comunicaciones o datos informáticos. Así, el juez puede ordenar esta medida, previa solicitud fundada por el fiscal. En este mismo artículo se refiere a la grabación de estas.

El Código Orgánico Procesal Penal venezolano de 2012 en su sección cuarta —"De la ocupación e interceptación de correspondencia y comunicaciones"— contiene el artículo 205, titulado "Interceptación o grabación de comunicaciones privadas". Así, podrá disponerse, conforme a la ley, la interceptación o grabación de comunicaciones privadas cuyo contenido se transcribirá y agregará a las actuaciones.

En una modificación de 2011 hecha al Código Procesal Penal colombiano, su artículo 235, sobre interceptación de comunicaciones telefónicas y similares, dispone que el fiscal podrá ordenar, con el único fin de buscar elementos materiales probatorios y evidencia física, que se intercepten mediante grabación magnetofónica o similares las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético, cuya información tengan interés para los fines de la actuación.

La Ley Especial sobre Intervenciones de las Comunicaciones Privadas de Honduras (2012) define en su artículo 3 la intervención de comunicaciones, señalando que es una técnica especial de investigación que consiste en el procedimiento a través del cual se escucha, capta,

registra, guarda, graba u observa, por parte de la autoridad, una comunicación que se efectúa por cualquier tipo de transmisión, emisión o recepción de signos, símbolos, señales escritas, imágenes, sonidos, correos electrónicos o información de cualquier naturaleza o por cualquier medio o tipo de transmisión.

El Salvador también cuenta con una les especial sobre intervenciones telefónicas (2010). En el artículo 13, sobre ejecución de la intervención, se indica que se grabarán y conservarán íntegramente y sin ediciones las telecomunicaciones de la persona o personas investigadas, mediante los mecanismos que la técnica señale y conforme a la autorización judicial.

La ley especial de crimen organizado de Nicaragua (2010) contempla en su capítulo VIII —"De la interceptación de comunicaciones"— que los jueces, previa petición, podrán autorizar impedir, interrumpir, interceptar o grabar comunicaciones, correspondencia electrónica, otros medios radioeléctricos e informáticos de comunicaciones fijas, móviles, inalámbricas y digitales o de cualquier otra naturaleza, únicamente para los fines de investigación penal. Luego, el artículo 213 de su Código Procesal Penal de 2014 trata sobre las intervenciones telefónicas.

Respecto a la legislación actualizada mexicana, en 2016 la Ley Federal contra la delincuencia indica en su capítulo sexto —"De la intervención de comunicaciones privadas"— que la intervención de estas comunicaciones abarca todo un sistema de comunicación o programas que sean fruto de la evolución tecnológica que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos, que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación. Luego, el artículo 18 determina las comunicaciones privadas que pueden ser objeto de intervención. El artículo 294 del Código de Procedimientos Penales (2014) también se refiere a este punto.

Brasil ha legislado al respecto en el Código Procesal Penal, cuerpo normativo que en una reforma de 2019 incluyó a la interceptación telefónica, de flujo de comunicaciones en sistemas de informática y telemática o de otras formas de comunicación, ello en las definiciones preliminares, al referirse a los jueces de garantía y sus funciones de autorización de medidas intrusivas.

Otra materia relevante es la relativa a la recolección de información, incluyendo la interceptación, con fines de inteligencia. Chile recoge en la Ley 19.974 de inteligencia (2004) los procedimientos especiales de obtención de información, que incluyen la intervención de comunicaciones, la intervención de sistemas y redes informáticos, la escucha y grabaciones electrónicas, y la intervención de sistemas tecnológicos destinados a procesar comunicaciones o información. En Paraguay, la Ley que crea el Sistema Nacional de Inteligencia (2014) sigue la misma línea que Chile, estableciendo un listado de procedimientos de obtención de información especiales, siendo estos excepcionales y requiriendo autorización judicial. Los cuatro procedimientos detallados en esta ley son los mismos listados en las dos leyes mencionadas. En Uruguay, la Ley Nº 19.696 de 2018, del Sistema Nacional de Inteligencia del Estado, incluye las mismas medidas que la ley de Chile y con similar redacción.

Estas medidas recientemente expuestas, en virtud de los estándares internacionales de protección de derechos humanos requieren cumplir con los principios de legalidad, objetivo legítimo, necesidad, proporcionalidad y existencia de una autoridad judicial competente, entre otros.

De la revisión de la Ley Federal contra la delincuencia organizada mexicana, la intervención de comunicaciones privadas está regulada por ley, se solicita a una autoridad judicial y requiere su autorización. Debe ser realizada en los términos aprobados por el juez o jueza. Esta solicitud debe estar debidamente fundamentada y la interceptación tiene un plazo para efectuarse; a su vez, está limitada (se debe "precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos y, en su caso, la denominación de la empresa concesionaria del servicio de telecomunicaciones a través del cual se realiza la comunicación objeto de la intervención"). También se señala que se puede solicitar cuando el Ministerio Público considere que sea necesaria, expresando el objeto y necesidad de esta. Para complementar esto, el Código de Procedimientos Penales establece que requiere autorización judicial previa en tanto afectan derechos consagrados en la Constitución. Este Código contiene normas similares a las de la intervención en la ley especial ya señalada, y reitera los requisitos de necesidad y delimitación del objeto de la medida.

En El Salvador, la ley especial para la intervención de las telecomunicaciones establece expresamente sus principios en el artículo 2. Allí contempla la jurisdiccionalidad ("Sólo podrán intervenirse las telecomunicaciones previa autorización judicial, escrita y debidamente motivada, en los términos de la presente Ley"), proporcionalidad, reserva y confidencialidad, temporalidad y limitación subjetiva ("La intervención debe recaer únicamente sobre las telecomunicaciones y medios de soporte de las personas presuntamente implicadas en el delito, ya sean sus titulares o usuarios habituales o eventuales, directa o indirectamente, incluidas las telecomunicaciones por interconexión. La intervención también puede recaer sobre aparatos de telecomunicaciones y otros medios de soporte abiertos al público"). Delimita la aplicación de la medida a un listado de delitos contenido en la ley, establece condiciones y detalla su ejecución. También, se refiere al control judicial de la intervención, señalando que el juez autorizante deberá controlar que la intervención se efectúe en los términos determinados en ley y en las condiciones establecidas en la resolución.

En el caso hondureño se parte de la base del reconocimiento de los derechos fundamentales de quien estará sometido a la medida. De este modo, en los considerandos del decreto que contiene la ley de intervención de comunicaciones se explaya sobre el derecho a la intimidad, su reconocimiento internacional y nacional, que la restricción a derechos debe ser solamente mediante mandato judicial y ajustándose a la ley. Además, dentro de la parte considerativa se refiere al combate de la perpetración de delitos (o su disminución), de esta forma, es posible pensar que esto se reconoce como lo que motiva a la regulación de la intervención.

Esta ley define una serie de principios tales como proporcionalidad, necesidad e idoneidad, confidencialidad, reserva jurisdiccional (la intervención sólo podrá autorizarse por el órgano jurisdiccional competente, de manera escrita, motivada y en los términos de esta ley). Se regula la autorización, la solicitud y su contenido, entre otros.

La regulación nicaragüense es más breve. En este sentido, indica que la interceptación de comunicaciones se realizará a solicitud expresa y fundada del Fiscal General de la República o del Director General de la Policía Nacional, y será autorizada por los Jueces del Distrito en lo Penal. Establece un plazo para la autorización y el contenido de esta que delimita su aplicación.

En Colombia se establece que la intervención de las comunicaciones debe ser fundada y por escrito, y se efectuará con único objeto de buscar elementos materiales probatorios y evidencia física. Lo más notorio es que está regulada dentro de las "Actuaciones que no requieren autorización judicial previa para su realización". Ello no significa que no participa una autoridad judicial, sino que lo hace en una audiencia de control de la legalidad posterior, en la cual el juez de control de garantías realizará una revisión de legalidad sobre lo actuado.

La normativa ecuatoriana también establece requisitos para la medida de intervención de comunicaciones, tales como autorización judicial previa, solicitud fundada, existencia de indicios que resulten relevantes a los fines de la investigación (los cuales se establecen en el Código), plazo para la interceptación y confidencialidad. Además, indica que "quedan prohibidas la interceptación, grabación y transcripción de comunicaciones que vulneren los derechos de los niños, niñas y adolescentes, especialmente en aquellos casos que generen la revictimización en infracciones de violencia contra la mujer o miembros del núcleo familiar, sexual, física, sicológica y otros".

La ley de inteligencia paraguaya, que contempla las tres medidas intrusivas analizadas, contempla los siguientes principios: respeto al ordenamiento jurídico, respeto al régimen democrático, respeto a los derechos constitucionales, autorización judicial previa, proporcionalidad, reserva y de la utilización exclusiva de la información. En refuerzo de lo anterior, destina un título a la protección de derechos y garantías. Otro punto destacable es que señala la excepcionalidad de estos procedimientos investigativos, solo siendo procedentes en los casos en que los órganos e instituciones del Sistema Nacional de Inteligencia no puedan obtener dicha información por fuentes abiertas, y esta debe ser estrictamente indispensable para el cumplimiento de una serie de objetivos que se expresan en dicha ley.

La ley de inteligencia uruguaya establece los principios de esta en su artículo segundo, disponiendo que los órganos integrantes del Sistema Nacional de Inteligencia de Estado desarrollarán sus actividades actuando bajo el más estricto cumplimiento de la Constitución de la República y de los principios del régimen democrático republicano de gobierno, en pleno respeto a los derechos humanos. Más adelante se refiere expresamente al principio de juridicidad y a la ponderación. El artículo 6 se titula derechos, deberes y garantías, en el cual se

reitera que el actuar del sistema Nacional de Inteligencia de Estado y las actividades de sus integrantes deberán ajustarse estrictamente a las disposiciones contenidas en la Sección II de la Constitución de la República, Leyes y Convenios internacionales adoptados por el Estado en materia de protección a los derechos humanos y garantías de sus habitantes. Luego, sobre los procedimientos especiales de obtención de información señala que requieren de autorización judicial.

Venezuela, en el artículo 205 de su Código Orgánico Procesal Penal, establece que la medida de interceptación podrá disponerse conforme a la ley. Además, el ente persecutor la solicitará de forma razonada al juez de control, especificando, entre otros, el delito que se investiga y la duración.

El Código argentino de 2019 inicia estipulando los principios y garantías generales donde se señala la protección de la intimidad y la privacidad, la restricción de los derechos fundamentales (lo cual debe ejercerse en conformidad con los principios de idoneidad, razonabilidad, proporcionalidad y necesariedad) y la motivación de las decisiones judiciales, entre otros. Sobre la medida de interceptación, se regula la autorización de la medida, la cual debe ser solicitada por el Ministerio Público Fiscal por escrito o en forma oral, especificando, entre otros, la finalidad de esta.

En Brasil, La modificación procesal de 2019 sobre los jueces de garantía establece que estos estarán a cargo de velar por la legalidad de la investigación penal y la salvaguarda de derechos individuales. Hace también mención a la autorización judicial previa de ciertas medidas dentro de las cuales se encuentra la interceptación.

En suma, todas las normativas dictadas en el periodo en estudio contemplan, de manera más restringida o amplia, requisitos para la ejecución de las medidas de intervención, lo cual significa un resguardo de los derechos respecto de quién se aplican aquellas. Aunque, es posible observar que la solicitud fundada/motivada, la autorización judicial y su consagración legal son los elementos mínimos de cada una de estas. También es común que se expresen los principios que rigen a estas medidas, dentro de los cuales están la proporcionalidad y la protección de derechos fundamentales, por señalar algunos.

Cifrado

Los individuos pueden optar por sistemas de cifrado para resguardar su privacidad ante las intromisiones externas, ya sea públicas o privadas, y en general esto no es materia de autorización o prohibición legal. Por el contrario, es comúnmente aceptado como una práctica necesaria de seguridad, tanto respecto de las comunicaciones (es decir, información en tránsito) como de los datos almacenados en dispositivos personales o de instituciones públicas y privadas (es decir, información en reposo). Esto se ha hecho especialmente importante para los defensores de los derechos humanos, activistas, periodistas y otros que pueden ser objeto de vigilancia y persecución en base a su labor. Los países que en la década en estudio se han referido expresamente a cifrado son: Colombia (2013), Cuba (2011, derogado en 2019), Honduras (2012) y El Salvador (2010).

En Colombia, señala el artículo 44 de la Ley Estatutaria 1621 que los operadores de servicios de telecomunicaciones deberán ofrecer a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia, un medio de transporte que permita llamadas de voz encriptadas, a un costo más utilidad razonable, y para un número específico de usuarios en condiciones que no degraden la red del operador ni la calidad del servicio que se presta. En este caso, se otorga el derecho de acceso al cifrado por parte de los sistemas de inteligencia exclusivamente. Por el contrario, en el caso de "equipos de comunicaciones que usan el espectro electromagnético", como los teléfonos celulares, tienen en principio prohibido el envío de "mensajes cifrados o en lenguaje ininteligible" (Ley 418 de 1997, prorrogada hasta 2022).

El artículo 21 de la Ley de Interceptación de Comunicaciones en El Salvador señala que, en un proceso de intervención que recaiga sobre material protegido (por cifrado, contraseña u otro motivo similar) puede ser conservado hasta la traducción o interpretación. Igualmente, define a esta, destacando su finalidad de hacer inaccesible o ininteligible a quienes no se encuentran autorizados para tener acceso a una comunicación. Similarmente, en la Ley Especial de Intervenciones Telefónicas de Honduras de 2012 se define al cifrado como una capacidad técnica.

Finalmente, el año 2011 en Cuba se estableció la obligación de aprobación oficial para usar cualquier tipo de aplicación o servicio por una red privada que involucre cifrado de la información transmitida, mediante reglamento. La medida se derogó en 2019.

Delitos contra la intimidad

Tres aspectos generales son clave en relación con la sanción penal de las infracciones a la vida privada o la intimidad. Por una parte, existen reglas preexistentes sobre delitos contra la intimidad que muy variablemente podrían o no aplicarse a infracciones en el entorno digital, como ocurre con la obtención o la diseminación de imágenes o información privada. En segundo lugar, existen otras aproximaciones que, en lugar de atender a bienes jurídicos vinculados a la intimidad, se refieren a la forma de comisión, como ocurre en la regulación de ciberdelitos con objetos de ataque que puedan consistir de información privada. Finalmente, existen múltiples esfuerzos legislativos por actualizar todas esas normas.

La difusión no consentida de imágenes íntimas (a menudo tratada en medios de comunicación como "pornovenganza") ha sido una conducta ampliamente reportada en esta década. El activismo ha sido fundamental para dar visibilidad a esta problemática y producir cambios legales. De los diecinueve países en estudio, varios de estos tipifican delitos de difusión de imágenes con contenido sexual o tomadas en recinto privado. Esa tipificación es muy variada en contenido y alcance, dado que no todas las reglas aplicables son necesariamente de la década en estudio. A la vez, esa dispersión está condicionada por la antigüedad de las reglas penales o por el poco reconocimiento político de estos casos, no contemplando la totalidad de material que puede ser difundido, o sin referencia a contenido sexual (más bien general, que importe violación de la intimidad a nivel genérico), que es parte del carácter de violencia de género común a estas acciones. En algunos casos, se considera un lugar específico de la producción del material difundido (espacios privados) como requisito del tipo penal, y no se refiere a medios electrónicos.

No obstante, existen países donde a partir de las reglas penales pueden configurarse hipótesis, aunque reducidas, respecto de la difusión no consentida de contenido sexual o imágenes íntimas.

En Perú, el artículo 154-B del Código Penal penaliza expresamente la difusión de imágenes y materiales audiovisuales con contenido sexual. En El Salvador, la tipificación del delito de revelación indebida de datos o información de carácter personal incluye imágenes, video, audio y otros (dentro de las cuales podrían ser contenido íntimo). Ecuador contempla el delito a la violación a la intimidad, donde penaliza la difusión y publicación de voz, audio y video. Diversos estados de México aprobaron el proyecto de ley Olimpia. República Dominicana, en su Código Penal, castiga la transmisión sin consentimiento de la imagen de una persona que se encuentre en un recinto privado, por lo que podría tratarse de imágenes íntimas.

El reconocimiento de la difusión no consentida de contenido íntimo ha sido tendencia durante la década, presentándose diversos proyectos de ley que buscan tipificarla como delito especial. El elemento común es la carencia de consentimiento de uno de los partícipes del acto íntimo. En Chile, el proyecto considera expresamente internet y en México el ciberacoso es explícitamente reconocido. Colombia incorpora una agravante en caso de que la víctima sea mujer.

A diciembre de 2019, distintos estados de México aprobaban la llamada Ley Olimpia, cuyo nombre proviene de la activista Olimpia Coral Melo.[7] El propósito es reconocer la difusión de contenido íntimo sin consentimiento como delito contra la intimidad, reconocer el ciberacoso como delito que general violencia sexual en internet. Entre los estados que adoptaron la ley se encuentra Ciudad de México, Aguascalientes, Baja California Sur, Chiapas, Coahuila, Guanajuato, Guerrero, Estado de México, Nuevo León, Oaxaca, Puebla, Querétaro, Veracruz, Yucatán y Zacatecas. Organizaciones basadas en la Ciudad de México se expresaron con preocupación por la aprobación de reglas penales entendidas como deficientes para prevenir la revictimización y resguardar derechos fundamentales.[8]

En 2019, se inició en Argentina el primer caso judicial sobre difusión de contenido íntimo.[9] Además, este acto se incluyó en la reforma del Código Penal de ese mismo año, definido como la "difusión sin consentimiento de imágenes o grabaciones de audio de naturaleza sexual producidas en la intimidad".[10]

En 2018, se presentó en Chile un proyecto de ley sobre difusión sin consentimiento de imágenes íntimas, que hoy continúa en discusión con algunos cambios. En principio, buscaba sancionar a quien "difunda o publique a través de Internet o cualquier otro medio electrónico imágenes de contenido o connotación sexual que se hayan obtenido con ocasión de la vida privada de la pareja y, sin el consentimiento de uno de ellos. Los administradores de sitios de internet que no bajen estas imágenes serán sancionados con la misma sanción".[11]

En Colombia se presentó en 2019 un proyecto de ley contra la difusión no consentida de imágenes íntimas, que sancionaría a quien "comparta material íntimo: videos, fotos, documentos, sin consentimiento de la persona afectada", con pena agravada si la víctima fuere mujer,[12] recogiendo así el componente de género detrás de esta conducta. El Código Integral Penal Ecuatoriano

7 El Sol de México. ¿De qué se trata la Ley Olimpia? 03 de diciembre de 2019. Disponible en: https://www.elsoldemexico.com.mx/mexico/justicia/de-que-se-trata-la-ley-olimpia-violencia-digitial-porno-venganza-ciberacoso-mujeres-coral-melo-4539259.html

8 Notoriox. "Preocupa a R3D y ARTICLE 19 aprobación de Ley Olimpia", 7 de diciembre de 2019. Disponible en: https://notoriox.com/preocupa-a-r3d-y-articulo-19-aprobacion-de-ley-olimpia/

9 Infobae, "Pornovenganza y Sextorsión: Arranca hoy el primer juicio en el país por difundir material sexual íntimo", 21 de noviembre de 2011. Disponible en: https://www.infobae.com/sociedad/policiales/2019/11/21/pornovenganza-y-sextorsion-arranca-hoy-el-primer-juicio-en-el-pais-por-difundir-material-sexual-intimo/

10 "Pornovenganza: nuevo delito incluido en la reforma del Código Penal", 11 de enero de 2019. Disponible en: https://www.argentina.gob.ar/noticias/pornovenganza-nuevo-delito-incluido-en-la-reforma-del-codigo-penal

11 Chile. 2018. Proyecto de Ley Delito de Pornovenganza. Disponible en https://observatoriolegislativocele.com/chile-proyecto-de-ley-delito-de-pornovenganza-2018/

12 N+1, "Colombia penará la "pornovenganza": hasta 8 años de cárcel para quienes divulguen contenido sexual por despecho", 29 de agosto de 2019. https://nmas1.org/news/2019/08/29/colombia-carce-pornovenganza

(2014, modificado en 2017) contiene disposiciones atingentes a este subcapítulo.[13]

Separadamente, es necesario analizar dos delitos que están relacionados: el delito de acceso no autorizado de datos y la difusión de datos personales. No son lo mismo, pero la obtención ilícita de información puede conllevar una futura divulgación, ya sea públicamente como a terceros interesados. La penalización del acceso no autorizado de datos no es necesariamente tendencia de esta década, pero ha habido una serie de casos de fuga de datos en este periodo en la región que ha hecho que este delito esté en la discusión pública. Así, por señalar algunos casos, en 2016 la cadena de hoteles Hyatt fue objeto de robo de dato de sus huéspedes en Argentina, Chile, Brasil, Panamá y México.[14] Luego, el blog de F-Secure en 2019 hizo un mapa de ataques cibernéticos en Latinoamérica donde resaltan países como Perú, Chile y México.[15]

Los países que en esta década incluyeron norma sobre castigo al acceso no autorizado de datos son Perú (2013) y Salvador (2016). Perú lo tipifica dentro de la ley de delitos informáticos de forma expresa y no dentro de un delito más general. Nicaragua lo regula especialmente dentro del Código Penal ("acceso y uso no autorizado de datos").

Por otra parte, la difusión de datos personales está tipificada como delito en algunos cuerpos normativos latinoamericanos, como es el caso de República Dominicana, Perú, El Salvador y Ecuador. Perú, a su vez, también penaliza el tráfico ilegal de datos personales. El Salvador cuenta con la "Ley Especial Contra los Delitos Informáticos y Conexos" de 2016 que trata mayoritariamente estos temas. El artículo 337 del Código Penal dominicano de 2014 castiga el atentado contra la intimidad de la vida privada.

Perú legisló al respecto durante la década, por medio de su ley de delitos informáticos (2013 y modificada en 2014) y el Código Penal, que en 2014 añadió el artículo 154 A, sobre tráfico ilegal de datos personales. Esto da cuenta de una creciente preocupación normativa, desde distintos ángulos, por la protección mediante sanciones penales de información privada.

---

13 Ecuador. 2014. Código Integral Penal. .

14 We live security. 2016. https://www.welivesecurity.com/la-es/2016/01/15/roban-datos-huespedes-hyatt-paises-latinoamerica/

15 F-Secure. 2019. https://blog.f-secure.com/es/mapa-de-los-ataques-ciberneticos-en-latinoamerica-2018/

Mandatos de registro de identidad en teléfonos

A lo largo de las últimas décadas, varios países de la región han mantenido o han intentado instaurar mandatos generales de registro de identidad en relación con el uso de teléfonos móviles de prepago. En estos casos, se argumenta usualmente que dicha medida está dispuesta para combatir delitos tales como el robo de teléfonos. No obstante, se ha asociado el uso de números no registrados para la comisión de varios ilícitos, por ejemplo, estafas, fraudes, comunicaciones entre grupos delictuales, narcotráfico, entre otros. En base a esto, distintos países han optado por mantener un registro de todos los usuarios de telefonía mayores de edad, con miras al combate de estas problemáticas, pudiendo rastrear a quien se comunica mediante ese equipo. Ha habido críticas ante la calidad que pueden tener estos registros y a la compleja situación a la cual puede exponerse a un usuario ante el robo de su dispositivo.

Ciertos países de la región han decidido disponer la obligatoriedad del registro la tarjeta SIM de los usuarios de servicios de telefonía. Las tarjetas SIM son de suma relevancia, puesto que guardan una serie de datos de su usuario, como el número de teléfono, el operador y otros datos como información de contactos, fotos y cuenta bancaria.[16] De este modo, el registro de una tarjeta SIM va más allá de uno que asocie un teléfono a un usuario, dado que aun si este cambia de teléfono,[17] normalmente la tarjeta perdura, siguiendo a su portador.

Los siguientes países de la región contemplan (o contemplaron) medidas de registro de números de prepago: México, Costa Rica, Guatemala, El Salvador, Cuba, Argentina, Perú (2004), Colombia y Uruguay. Cabe destacar que en México se abandonó esta medida, pero se ha discutido implementarla nuevamente.[18] En Chile se presentaron proyectos de ley sobre la materia, pero no se concretizaron. De manera similar, no se encontró legislación relevante en Costa Rica sobre esta materia, pero existe una plataforma para "Registro de Prepago"[19] a cargo de la Superintendencia de Telecomunicaciones (SUTEL).

En Guatemala existe la Ley de equipos terminales móviles (2013) y los prepagos deben re-

16 Augusto Peña. ¿Qué información guarda tu tarjeta SIM? El internacional, 11 de marzo de 2019. Disponible en: https://www.eluniversal.com.mx/techbit/que-informacion-guarda-tu-tarjeta-sim

17 En Argentina se ha estimado que las personas lo hacen cada dieciocho meses. Ver La Nación, ¿Con qué frecuencia reemplazan los argentinos sus celulares? 21 de noviembre de 2016. Disponible en: https://www.lanacion.com.ar/tecnologia/cada-cuanto-tiempo-cambian-los-argentinos-sus-celulares-nid1958175

18 Digital Policy Law, "México alista otra iniciativa para registrar las tarjetas SIM prepago, tras intento fallido de 2009", 18 de enero de 2020. Disponible en: https://digitalpolicylaw.com/mexico-alista-otra-iniciativa-para-registrar-las-tarjetas-sim-prepago-tras-intento-fallido-de-2009/

19 Digital Policy Law, "Apenas una sexta parte de las líneas prepago está registrada en Sutel", 23 de julio de 2019. Disponible en: https://digitalpolicylaw.com/apenasuna-sexta-partedelaslineas-prepagoesta-registrada-en-sutel/

gistrarse.[20] Argentina norma al respecto en el Reglamento de calidad de los servicios de telecomunicaciones (2013) y en octubre de 2018 se lanzó "Tu línea es tuya", iniciativa impulsada por el Ministerio de Seguridad, Ente Nacional de Telecomunicaciones (ENACOM) y el Ministerio de Comunicaciones, sobre registro obligatorio de prepagos.[21] También, está el Decreto 274/14 de 1 octubre de 2014 en Uruguay, que regula el registro de prepagos.

En Guatemala, la ley de equipos terminales móviles de 2013, en su artículo 14, establece que: "los usuarios que adquieran una tarjeta SIM, deberán exhibir ante el vendedor su documento de identificación personal en el que se verifique su mayoría de edad; en el caso de los extranjeros, su pasaporte vigente. Es obligación del usuario o comprador que adquiere una tarjeta SIM, proporcionar al vendedor una copia física o electrónica de su documento legal de identificación personal, en esta copia que queda en posesión del vendedor se debe anotar el número de SIM, es decir el número de teléfono que está adquiriendo el usuario, o suscribir en formulario respectivo que podrá ser electrónico los datos antes mencionados, debiendo conservar el vendedor esos archivos o documentación por un período de tres (3) años".

En Nicaragua, el artículo 45 del Reglamento de la Ley de prevención, investigación y persecución del crimen organizado (2010), referido al registro oficial e identificación de usuarios, establece que en este se incluye a las empresas o personas naturales que enajenen de cualquier forma teléfonos móviles y tarjetas SIM. De este modo, se registran a los vendedores de estas tarjetas. Luego, a este registro tendrán acceso las autoridades de policía y el Ministerio Público en el ejercicio de sus funciones y atribuciones.

20 Guatemala, "Cómo y quiénes deben registrar su celular en Guatemala para que no lo suspendan", 5 de octubre de 2016. Disponible en: https://www.guatemala.com/noticias/sociedad/como-y-quienes-deben-registrar-su-celular-en-guatemala-para-que-no-lo-suspendan.html

21 Argentina. Tu línea es tuya. Disponible en https://www.argentina.gob.ar/registra-tu-linea/

Reglas sobre retención de datos de comunicación

Además del registro de usuarios asociados a un número o servicio de telefonía y de las normas de interceptación de comunicaciones, es necesaria la revisión de aquellos casos en los que se establecen medidas de conservación o entrega de datos sobre comunicaciones. No solamente en relación con los datos asociados a comunicaciones telefónicas, como lo serían la duración de las comunicaciones o los números de los interlocutores, entre otros, sino también aquellos datos asociados a la navegación y la comunicación en internet.

El Decreto Nº 360 sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional de Cuba (2019) dispone implementar los mecanismos y procedimientos que aseguren la identificación del origen de las conexiones, incluidas las conmutadas, así como su registro y conservación por un tiempo no menor a un año (artículo 87). Señala además la obligación de facilitar a las autoridades competentes de los registros de las conexiones y cooperar en la investigación de violaciones de las normas establecidas y los incidentes de seguridad.

El artículo 39 de la Ley Especial de Intervenciones Telefónicas de Honduras (2012) mandata a las compañías que brindan servicios telefónicos a guardar los datos de todas las conexiones de cada usuario por el plazo de cinco años. Se refiere a teléfonos fijos y móviles.

La Ley de crimen organizado (2010) de Nicaragua señala en su artículo 65 que se las empresas privadas o públicas prestadoras de los servicios de comunicación telefónica, informática o de otra naturaleza electrónica, y otras que utilicen el espectro electromagnético y radioelectrónico, deben llevar registro oficial de los usuarios o clientes que los utilicen. Es destacable que incluye tanto a las comunicaciones telefónicas como las realizadas a través de internet.

En Venezuela, el artículo 10 de la providencia administrativa 171 de 2017 se refiere a los registros de servicios de datos, sobre lo cual regula que los operadores de telefonía móvil o fija deben almacenar y disponer de un registro de sus abonados que contenga elementos como direcciones IP de emisor y receptor, fecha y hora de conexión, coordenadas geográficas, etc. Los operadores deben proporcionar esta información al momento de ser solicitada.

En Perú se normó al respecto el año 2015, mediante el Decreto Legislativo 1182. En las disposiciones complementarias finales de este documento se dispuso la conservación de los datos derivados de las telecomunicaciones. Así, los concesionarios de servicios públicos de telecomunicaciones y las entidades públicas relacionadas con estos servicios deben conservar durante los primeros doce meses en sistemas informáticos que permitan su consulta y entrega en línea y tiempo real.

En Colombia, la Ley Nº 1621 sobre colaboración con operadores de servicios de telecomunicaciones de 2013 establece en el artículo 44 que los operadores de servicios de telecomunicaciones estarán obligados a suministrar a los organismos de inteligencia y contrainteligencia el historial de comunicaciones de los abonados telefónicos vinculados, los datos técnicos de

identificación de los suscriptores y la localización de las celdas en que se encuentran estas terminales, entre otras.

Finalmente, el Marco Civil de Internet de Brasil (2014) dispone en su artículo 15 que el proveedor de aplicaciones de internet constituido como persona jurídica y que ejerza esa actividad de manera organizada profesionalmente y con fines económicos deberá mantener los respectivos registros de acceso a aplicaciones de internet en ambiente controlado por un plazo de seis meses.

En Paraguay no existe normativa relevante al respecto. Se rechazó en 2015 el proyecto de ley que buscaba obligar a los proveedores de servicios de internet la conservación de los datos de las comunicaciones (Díaz, 2017).

En suma, de los diecinueve países en estudio, siete contienen normas sobre registro de comunicaciones telefónicas o digitales dictadas durante la década en estudio.

Normas sobre biometría

Aunque a lo largo de la década existió una fuerte tendencia a incorporar y regular aspectos relacionados con la biometría en toda América Latina, su alcance fue más bien limitado a la regulación de usos dentro de procesos de investigación. Si bien sabemos que existe una utilización creciente de tecnologías biométricas con fines de identificación y verificación de identidad, especialmente con fines de vigilancia pública y de control en la provisión de servicios estatales,[22] incluyendo la creación de sendas bases de datos biométricos por parte de los Estados, buena parte de esa creciente utilización se hace sin modificaciones legales especiales. Allí donde ha existido modificación, ella no se ha concentrado en los aspectos más íntimamente vinculados con la digitalización de la información ni con la datificación de los individuos en su interacción con instituciones diversas.

Valga igualmente mencionar algunas de las modificaciones relevantes. En El Salvador, el Código Procesal Penal de 2009 (modificado en 2016) trata a las huellas digitales con relación a la identificación del imputado (artículo 83), la cual puede hacerse mediante este método. Luego, el artículo 187 trata sobre las pruebas de ADN. De la revisión del Código Procesal Penal de Honduras (1999) es posible encontrar una norma (artículo 107) sobre exámenes corporales y extracción de muestras del imputado. Este artículo fue incorporado en 2013. No se señalan ejemplos de estos exámenes y muestras. A su vez, en el Código Procesal Penal de Nicaragua (2014) resalta el artículo 238 sobre investigación corporal que contempla exámenes de fluidos biológicos y otras intervenciones corporales.

El Código Procesal Penal Federal argentino (2019) se refiere tanto a las huellas dactilares como al ADN. Respecto de las primeras, el artículo 66 sobre identificación y domicilio dispone que se puede identificar por datos personales, señas particulares e impresiones digitales (igualmente, contempla una mención a otros medios, que abre el artículo a mayor cantidad de datos biométricos). Por otro lado, el artículo 175 indica que, para individualizar una persona, se puede ordenar la obtención de ADN del imputado o de otra. En Colombia, el Código de Procedimiento Penal (2004) se pronuncia sobre datos biométricos después de una modificación dentro de la década en estudio. Así, el artículo 245 (añadido en 2018) se refiere a los exámenes de ADN del imputado o del indiciado. Se señala que estos (y otros datos que permitan identificación, tales como la huella digital) requieren orden expresa del fiscal. Con mayor especificidad está el artículo 251 sobre métodos de identificación señala al perfil genético o a las características morfológicas como las huellas digitales.

El Código Orgánico Integral Penal del Ecuador (2014) se refiere dentro de la toma de muestras a los datos genéticos de la siguiente forma: "obtención de muestras de fluidos corporales, componentes orgánicos y genético-moleculares".

---

22 Díaz, M. (2018). El cuerpo como dato. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf

Respecto del control de identidad, el artículo 55.2 del Código Procesal Penal de Uruguay de 2015 ordena que, si la persona no cuenta con los documentos para este control, la persona autorizará por escrito que se tomen sus huellas digitales, las que solo podrán ser utilizadas con fines identificatorios. El artículo 195 del Código Orgánico Procesal Penal de Venezuela de 2012 se refiere al examen corporal y mental del imputado en términos generales, sin dar ningún ejemplo ni caso específico.

La primera tendencia regional que queda a la vista es que no existen cuerpos normativos dedicados especialmente a regular la recolección y el uso de datos biométricos. De este modo, los artículos que tratan sobre este punto están contenidos en otros tipos de leyes. A la vez, allí donde existieron modificaciones, la utilización de las tecnologías se vuelve un aspecto más bien accesorio y sujeto a otras formas de control. La utilización cotidiana de biometría por órganos de vigilancia está excluida.

Los datos biométricos que se identificaron normados en mayor cantidad de Códigos fueron las huellas digitales. Sobre las huellas digitales, dentro de la década en estudio, estas están normadas en Uruguay, El Salvador, Argentina y Colombia. Como se vio, los casos son respecto de control de identidad e identificación. Esto es concordante con la definición de dato biométrico dada en la introducción, dentro de cuyas características se estableció su carácter identificatorio. El tratamiento de la huella digital es un dato que es único de cada persona, permitiendo una identificación del 100% con el sujeto investigado. Cabe destacar la norma uruguaya que establece el principio de finalidad de la toma de este dato biométrico dentro de su redacción (solo podrá ser utilizada para fines identificatorios).

A modo de cierre, en el presente estudio no encontramos ningún cuerpo regulatorio o norma sobre tecnologías de reconocimiento facial automatizado. Pese a la creciente tendencia al uso en espacios públicos de sistemas de vigilancia con esas capacidades, y del peculiar riesgo que el reconocimiento facial implica en tal sentido,[23] son apenas las normas constitucionales y las reglas legales existentes sobre datos personales y sobre facultades de las autoridades públicas las que estarían llamadas a regular o controlar esas utilizaciones.

---

23 Véase, por ejemplo, Reconocimientofacial.info, disponible en: https://www.reconocimientofacial.info

Resumen de hallazgos

Si hay algo que resalta del presente estudio es la actualización de determinados cuerpos normativos. Así, destacan la fecha de dictación de los Códigos Procesales Penales y leyes de protección de datos personales, siendo la mayoría de estos de la década en estudio. La actualización normativa también está presente en otro tipo de leyes especiales (como las de telecomunicaciones o crimen organizado), pero en menor medida. Los dos tipos de leyes mayormente actualizadas son de suma importancia, en tanto afectan directamente en los capítulos de datos personales, vigilancia y también, en menor medida, en el capítulo de comunicaciones. Lamentablemente, sobre normativa de datos biométricos existe menos regulación.

Con relación a datos personales, lo más destacable es que la mayoría de los países de la región tienen leyes especiales al respecto y aproximadamente un tercio de los que no regulan especialmente esta materia están en proceso de tenerla. El 77% de los países latinoamericanos que actualmente tienen ley de protección de datos la dictaron durante la década en estudio. Finalmente, existen incipientes tendencias a considerar la protección de datos personales como un derecho autónomo distinto a la privacidad o intimidad; a nivel judicial hay una tendencia a ver causas relacionadas al derecho al olvido.

Respecto de actividades de vigilancia e inteligencia y la normativa dictada en la década 2010-2020, el 58% de los países latinoamericanos cuenta con normativa sobre interceptación de comunicaciones que data de esta década, 47% sobre grabación de estas y dos países contemplan intervención de sistemas informáticos, ambas dictadas en este mismo periodo. En su mayoría, estas medidas se regulan en la legislación procesal penal de cada país, minoritariamente en leyes/reglamentos especiales de interceptación de comunicaciones, leyes de inteligencia y de crimen organizado. De los17 países que tienen normas sobre este punto, 12 tienen legislación actualizada durante la década en estudio. En promedio, alrededor del 50% de los países de la región regularon estas dos primeras medidas entre 2010-2020, mientras que la intervención de sistemas informáticos es una tendencia incipiente en las leyes de inteligencia de esta década.

Sobre los delitos contra la intimidad, si bien las leyes o proyectos de ley que castigan los hechos constitutivos del delito de difusión no consentida de material íntimo son una tendencia incipiente de la segunda mitad de la década, diversos Códigos Penales han penalizado la difusión o revelación de contenido o imágenes de carácter sexual, como un tipo penal más amplio que le podría contener. Otro delito de relevancia es el acceso no autorizado de datos, tipificado en la mitad de Latinoamérica, tanto en Códigos Penales como en leyes de delitos informáticos.

En lo referente a reglas sobre retención de datos personales o mandatos de registro de identidad en teléfonos, cabe destacar la tendencia del periodo 2010-2020 dentro de Latinoamérica sobre la imposición del registro de servicios de telefonía de prepago en el 42% de los dieci-

nueve países analizados. De manera similar, el 16% de estos países disponen el registro de tarjetas SIM. Ambas medidas se justifican, mayormente, en el combate contra el crimen. Por otro lado, el 37% de los países de la región contemplan normas sobre medidas de registro de comunicaciones telefónicas o digitales. De estos nueve países, cinco hacen mención expresa a comunicaciones en línea.

Finalmente, se estudiaron las normas sobre biometría. Primero, es destacable que la mayoría de las legislaciones que cubre esta materia está actualizada en la década 2010-2020, de este modo, el 59% de los Códigos Procesales Penales que tienen disposiciones al respecto entraron en vigor o fueron modificados en este periodo. Como punto general se analizaron los 19 países y se encontró que 16 recogen en su legislación normas sobre datos biométricos. Específicamente, el dato biométrico mayormente regulado es la huella digital (21%). Minoritariamente, algunos países regulan las pruebas de ADN (16%).

Identificación de desafíos

Protección de datos personales:

Considerando que sólo cinco países de los 19 en estudio reconocen a la protección de datos personales como un derecho autónomo, un primer desafío consiste en que los países lo consagren idealmente a nivel constitucional, para elevarlo en la cúspide de los sistemas jurídicos de cada país.

Si bien una acción judicial es primordial para hacer efectiva la protección de este derecho, antes de esto se debe instaurar una institucionalidad destinada a la protección de datos personales. Si bien excede lo estudiado en este trabajo, contar con una autoridad de control con potestades sancionatorias potenciaría la exigibilidad y cumplimiento de las disposiciones normativas, puesto que estando aquellas solo en el papel las hace poco efectivas.

Como se vio, una serie de países recoge completa o parcialmente los derechos arco. Se sugiere la adopción en un futuro de todos estos derechos y de la habilitación para los habitantes de cada país en estudio de canales de uso sencillo para hacerlos valer, por ejemplo, un formulario en el sitio web de la agencia estatal correspondiente.

Considerando la interconexión entre los países en la actualidad y la creciente atracción de la región como foco de negocios de grandes compañías, es necesaria la regulación de transferencia transfronteriza de datos, considerando que muchas industrias (como la farmacéutica, financiera o de tecnología, entre otros) manejan un amplio volumen de información personal. Es de los intereses económicos y sociales el fortalecimiento de los estándares y normas dispuestas a este flujo, velando por siempre exigir unas garantías iguales o superiores en el tratamiento a las que existen en cada país.

Vigilancia e inteligencia:

Se debe tener en cuenta que el 29% de la normativa regional es anterior al año 2010, por lo tanto, el primer paso necesario es la actualización legislativa. Según lo expuesto, un desafío es la dictación y actualización de leyes diferentes al Código Procesal Penal. La persecución penal del crimen organizado y los delitos tipificados dentro de las leyes de inteligencia suponen una fuerte investigación penal. Como se vio, las leyes de inteligencia de algunos países contemplan una serie de procedimientos especiales probatorios altamente intrusivos, no obstante, estos también estaban sujetos a estrictas condiciones. Considerando esto, es menester que cada país cuente con disposiciones sobre este tipo de medidas en las leyes especiales de persecución criminal, que puedan interferir mayormente con el derecho a la privacidad de las personas, estableciendo en detalle requisitos y garantías en caso de ser necesario su uso.

La consagración en términos generales sobre la intervención de comunicaciones es una ten-

dencia regional, mas no el establecimiento de un reglamento o ley especial dedicado a esta medida investigativa en particular. Estimamos como desafío que cada país elabore una norma aparte que complemente la medida dispuesta mayoritariamente en Códigos Procesales Penales, nuevamente, estableciendo mayores requisitos y condiciones de seguridad y de protección de los derechos del investigado.

Delitos contra la intimidad

Es positiva la tendencia de la segunda mitad de la década sobre penalizar la difusión no consentida de material íntimo, ya sea con leyes ya en efecto (como México) como también con la idea de legislar (Chile, por ejemplo). Considerando que en países como Colombia y México la discusión se estableció por casos de mujeres activistas afectadas por esta conducta es que es posible observar una tendencia regional en favor de la lucha contra esta forma de violencia. No obstante, es posible pensar que existe silencio respecto de estas situaciones en otros países de la región, por lo cual es un desafío futuro legislar y tipificarla como delito sancionado en leyes penales. Es interesante observar el caso colombiano en el cual se estableció como circunstancia agravante el hecho de ser una mujer víctima de este delito.

A su vez, algunos países penalizan el acceso no autorizado a bases de datos, hecho que debiese extenderse a toda la región. Sumado a esto, es necesario establecer estrictas medidas de seguridad que apoyen la defensa de los datos de cada persona

Retención de datos personales y registros de identidad en telefonía:

Existen argumentos para considerar medidas de registro de servicios de prepago y tarjetas SIM. No obstante, si ello se efectúa, deben establecerse medidas robustas de seguridad para la protección de estos datos, canales de actualización y un método eficiente para denunciar y bloquear estos dispositivos, considerando que muchas veces la misma medida de registro puede crear incentivos para la instauración de un mercado negro de equipos robados o el robo de estos para la comisión de delitos. De este modo, es un desafío lograr conjugar todos estos elementos en los casos es que los países estimen completamente necesarias las medidas de registro y, sobre todo, realizar un análisis de los factores positivos y negativos al momento de establecerlos, no sólo considerando el combate criminal, sino también las desventajas que pueden conllevar estas medidas.

Respecto del registro de comunicaciones, las leyes de cada país deben modernizarse e incorporar las comunicaciones digitales. Pocos países las regulan. A su vez, deben establecerse altos estándares de seguridad para la recolección y almacenamiento de esta información.

Biometría:

Es preciso que los países en estudio regulen con mayor detalle este punto, más allá de la recolección de muestras biológicas que está ampliamente cubierta en las legislaciones procesales penales latinoamericanas. Como se analizó, los datos biométricos regulados en específico que identificamos como tendencia son las huellas digitales y las pruebas de ADN, con una utilización creciente que supera las regulaciones específicas y parece estar cubierta por las reglas generales de protección de datos personales de carácter sensible. No todos los países regulan estos usos, así que un paso inicial debe ser ampliar la regulación de estas a toda la región en estudio. Además, actualmente existen otros tipos de datos biométricos que se registran y utilizan en la práctica, tales como el escaneo facial u ocular. Estos son ampliamente utilizados para la apertura de entradas, por ejemplo. Por esto, es necesario que Latinoamérica regule a la brevedad esta situación, de manera respetuosa de los derechos de las personas.


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina