LA CONSTRUCCIÓN DE ESTÁNDARES LEGALES PARA LA VIGILANCIA EN AMÉRICA LATINA

PARTE I: ALGUNOS EJEMPLOS DE REGULACIÓN ACTUAL EN AMÉRICA LATINA

SEBASTIÁN BECKER
J. CARLOS LARA
MARÍA PAZ CANALES

DERECHOS DIGITALES
América Latina

LA CONSTRUCCIÓN DE ESTÁNDARES LEGALES PARA LA VIGILANCIA EN AMÉRICA LATINA

PARTE I: ALGUNOS EJEMPLOS DE REGULACIÓN ACTUAL EN AMÉRICA LATINA

SEBASTIAN BECKER
J. CARLOS LARA
MARÍA PAZ CANALES

@ | DERECHOS DIGITALES
América Latina

Portada y diagramación: Javiera Méndez
Correcciones: Vladimir Garay
Septiembre de 2018.

Esta publicación fue posible gracias al apoyo de Global Partners Digital

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 de la libertad de expresión, el acceso a la cultura y la privacidad.

1. Introducción

Con una facilidad nunca antes vista, avanzadas tecnologías para la vigilancia de comunicaciones, de espacios y de individuos se encuentran disponibles para los Estados. Los servicios y dispositivos son ofrecidos por las compañías privadas que las comercializan alrededor del mundo a los Estados de nuestra región. Las leyes, incluso allí donde tienen principios claros para su aplicación, a menudo se quedan rezagadas frente al avance de la capacidad vigilante del Estado.

Para constatar el impacto de la tecnología en las capacidades de vigilancia, no hace falta una investigación en profundidad. Basta ver como en todo el mundo, y en particular en América Latina, los órganos estatales han comenzado a adquirir distintas tecnologías como cámaras de alta definición, cámaras con tecnología de reconocimiento facial, lectores biométricos de huellas dactilares, aeronaves no tripuladas y globos aerostáticos con videocámaras, software de vigilancia remota, IMSI-catchers, entre otras tecnologías. La razón clásicamente esgrimida es la necesidad de resguardar la seguridad pública o hacer más eficiente la acción de policías e investigadores criminales. Estas tecnologías son cada vez más invasivas y lesivas de los derechos humanos de las personas. En su uso, los estados deben también considerar que no puede existir verdadera seguridad pública sin respeto de los derechos humanos.

En el contexto latinoamericano, se han levantado múltiples voces sobre los peligros que trae consigo el uso de tecnologías para el ejercicio de los derechos humanos, particularmente estas en países de mayor inestabilidad socio-política. Chile no está exento de este escenario: recientes episodios como la implementación de programas de seguridad pública consistentes en la operación de drones y globos de vigilancia, dotados de cámaras de alta resolución, la fallida y polémica "Operación Huracán" y la vigilancia a que frecuentemente se encuentran sometidos dirigentes de la etnia mapuche, dan cuenta de la urgencia de iniciar un debate serio sobre estos temas.

En dicho contexto, surge la necesidad de abrir una conversación respecto de los estándares normativos que deben regir el uso de dichas tecnologías. Hoy, muchas de ellas se adquieren, despliegan e implementan en forma opaca, por vía meramente administrativa y sin un debate democrático que considere su impacto en el ejercicio de derechos fundamentales, tales como la protección de la privacidad, la libertad de expresión, el derecho a reunión pacífica y el derecho a no ser discriminado.

El propósito de esta investigación es relevar los estándares normativos que se han desarrollado a nivel comparado y en el sistema internacional de protección de los derechos humanos, que permitan identificar los elementos que debieran encontrarse presentes en un marco normativo para el uso de tecnologías de vigilancia en forma respetuosa de los derechos fundamentales. No con un ánimo de recoger y comparar normativas, sino de construir estándares accionables a partir de los cuales iniciar procesos de cambios normativos y prácticos en el uso de herramientas de vigilancia.

La investigación de las páginas siguientes no pretende ser exhaustiva ni agotar la discusión sobre las muchas aristas consideradas, donde existe vasta bibliografía nacida tanto de la academia como de investigadoras independientes, así como de la sociedad civil organizada.

Tampoco pretende dar por sentados los parámetros y estándares definitivos para una eventual regulación; por el contrario, se espera que este trabajo sea el punto de partida de una discusión que nos parece urgente y necesaria: cómo garantizar los derechos humanos ante el uso de tecnologías de vigilancia en la era digital.

La metodología del estudio consideró el levantamiento de legislaciones locales, revisión de jurisprudencia y se apoyó en la doctrina sobre cada uno de los puntos expuestos. Lo anterior, acompañado de la referencia a casos de estudio específicos conocidos a partir de hechos noticiosos, con el objeto de dar cuenta de algunas hipótesis que subyacen a la investigación. El informe pretende proveer hallazgos sobre los estándares que las normativas comparadas –que han sido objeto de revisión a la fecha– utilizan para regular la vigilancia, y constatar si es que éstos cumplen o no con los principios que desde Naciones Unidas y el Sistema Interamericano de Derechos Humanos recomiendan para precaver el respeto de los derechos humanos en su implementación.

Para lo anterior, se han escogido cinco áreas temáticas de estudio: (1) leyes que contemplan capacidades de inteligencia; (2) normativa que regula la interceptación de comunicaciones; (3) normativa que regula la retención de datos y metadatos por proveedores de servicios (ISPs); (4) normativa que regula la televigilancia; y, (5) normativa que regula el uso de biometría. Dichos acápites contienen una versión sintética sobre una investigación que englobó a legislaciones de Argentina, Brasil, Chile, Colombia, Guatemala y México. Un segundo texto explorará algunas normas ejemplares de países fuera de la región.

2. Vigilancia y privacidad

2.1. Protección de la privacidad en el ordenamiento jurídico

La privacidad en distintos ordenamientos jurídicos es protegida tanto a nivel constitucional como legal. La protección de la privacidad se ha erigido como un valor fundamental para las democracias modernas, dotado de sendas construcciones doctrinales para su reconocimiento como un derecho humano. No obstante, los límites de la privacidad en la era digital están en constante tensión dado que "*las tecnologías de la comunicación también han aumentado la capacidad de los gobiernos, las empresas y los particulares para realizar actividades de vigilancia, interceptación y recopilación de datos*".[1] Esa tensión se extiende a las implicancias normativas de la privacidad, tanto a nivel constitucional como legal.

No obstante lo anterior, existen varios esfuerzos a nivel global por proteger la privacidad en la era digital. Los órganos oficiales de protección de derechos humanos, a nivel internacional y regional, han realizado denodados esfuerzos por promover una noción de privacidad que se adecúe a los estándares necesarios para otorgar una efectiva protección a las personas en el contexto del uso de herramientas digitales. Lo anterior se desprende de que tanto la Convención Americana sobre Derechos Humanos (en adelante, CADH) en su artículo 11, como la Declaración Universal de Derechos Humanos (en adelante, DUDH) en su artículo 12,[2] y el Pacto Internacional de Derechos Civiles y Políticos (en adelante, PIDCP) en su artículo 17,[3] entre otros instrumentos, reconocen un derecho a la no interferencia arbitraria sobre la vida privada y familiar de la persona, su domicilio y su correspondencia, o al reconocimiento y respeto a la dignidad, integridad personal o reputación. De este modo, tanto la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) como la Relatoría Especial para la Privacidad de Naciones Unidas han emitido informes y declaraciones sobre la necesidad de proteger la privacidad en la era digital.

En el contexto chileno, la protección de la privacidad está recogida bajo dos fórmulas normativas. La primera es bajo el amparo del artículo 5° inciso 2° de la Constitución, que señala que:

> "El ejercicio de la soberanía reconoce como limitación el respeto a los derechos esenciales que emanan de la naturaleza humana. Es deber de los órganos del Estado respetar y promover tales derechos, garantizados por esta Constitución, así como *por los tratados internacionales ratificados por Chile* y que se encuentren vigentes".

De esta forma, la privacidad puede ser ejercida y protegida en suelo nacional, tanto por ciudadanas como por no ciudadanas, en nombre de los tratados internacionales que Chile ha suscrito.

Por otro lado, el artículo 19 establece que:

---

1 Naciones Unidas. Asamblea General. El derecho a la privacidad en la era digital. UN Doc. A/RES/68/167. 21 de enero de 2014. Párr. 2 .

2 "Artículo 12. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

3 "Artículo 17. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación (...) Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

> "La Constitución asegura a todas las personas: ...
> 4º. El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley;
> 5°. La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar solo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley".

La protección de la privacidad, tanto a nivel internacional como nacional, constituye un derecho humano. Lo anterior implica que los países firmantes de tratados internacionales deben cumplir con una serie de estándares necesarios para velar por la privacidad a su ciudadanía, esto implica, como lo ha señalado la Corte Interamericana de Derechos Humanos (Corte IDH):

> "a) el derecho a contar con una esfera de cada individuo resistente a las injerencias arbitrarias del Estado o de terceras personas; b) el derecho a gobernarse por reglas propias según el proyecto individual de vida de cada uno; c) el derecho al secreto respecto de lo que se produzca en ese espacio reservado con la consiguiente prohibición de divulgación o circulación de la información capturada, sin consentimiento del titular, en ese espacio de protección reservado a la persona; y d) el derecho a la propia imagen".[4]

De esta forma, los Estados tienen no solo la obligación de abstenerse de realizar actuaciones arbitrarias o ilegales, sino además de adoptar acciones positivas que impidan la vulneración de la privacidad.[5] Finalmente, se desprende tanto de los esfuerzos del sistema universal como del Sistema Interamericano de Derechos Humanos (SIDH) que cualquier clase de limitación al derecho a la vida privada debe superar el test de legalidad, proporcionalidad y necesidad.[6]

Teniendo claro el marco general de protección a la privacidad, podemos dar paso a la descripción y configuración de nuestro objeto de estudio: la vigilancia en un marco normativo respetuoso con los derechos humanos. En el siguiente acápite se revisará cómo es que la privacidad se configura y protege en marcos normativos que permiten y desean la vigilancia sobre la ciudadanía. Para ello será necesario abordar y explorar normativas nacionales y extranjeras que regulen (y autoricen) la vigilancia con el objeto de encontrar mecanismos que permitan equilibrar, por un lado la privacidad de las personas y por el otro, las facultades de vigilancia de los Estados. De esta manera, será posible extraer prácticas concordantes con los derechos humanos y detectar técnicas normativas incongruentes con los sistemas de protección a los derechos fundamentales.

---

4 Relatoría Especial para la Libertad de Expresión (2017). "Estándares para una Internet libre, abierta e incluyente", Comisión Interamericana de Derechos Humanos, OEA/Ser.L/V/II CIDH/RELE/INF.17/17. párr. 191.

5 Corte IDH. Caso Fontevecchia y D'Amico vs. Argentina. Sentencia de 29 de noviembre de 2011. Fondo, Reparaciones y Costas. Serie C Nº 238. Párr. 49.

6 Véase Naciones Unidas. Asamblea General. El derecho a la privacidad en la era digital. UN Doc. A/RES/68/167. 21 de enero de 2014. Párr. 22-27 y RELE, Ob. cit. párr. 193.

3. Situación normativa de las facultades de vigilancia en América Latina

3.1. Criterios jurídicos emanados del Sistema Interamericano aplicables a la implementación de tecnologías de vigilancia

El artículo 11.2 de la CADH protege a la vida privada de injerencias arbitrarias, es decir, existe un ámbito personal que debe estar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública.[7] Estos ámbitos incluyen el domicilio, la vida familiar[8] y las comunicaciones,[9] entre ellas, las que se producen a través de internet.[10] De la misma forma, la CADH obliga a los Estados parte no solo a la abstención de injerencias arbitrarias y/o ilegales sino además a garantizar mediante acciones positivas el derecho a la vida privada.[11]

La implementación de sistemas de vigilancia no solo permite una erosión de la privacidad de las personas, sino además la vulneración concreta de otros derechos humanos. Tanto el Alto Comisionado de Naciones Unidas para los Derechos Humanos como la CIDH han señalado que la interceptación de comunicaciones digitales o la recopilación de datos personales pueden afectar tanto a la libertad de expresión, de reunión y asociación pacífica, como al derecho a la vida familiar.[12] Es por ello que mecanismos como la televigilancia, interceptación de comunicaciones, retención de data y metadatos y/o la vigilancia mediante tecnología biométrica han sido catalogados como amenazas tanto al catálogo de derechos humanos como al sistema democrático de derecho.[13]

El SIDH ha establecido un test tripartito para verificar la adecuación al marco interamericano de derechos humanos de las injerencias estatales o no estatales en la vida privada mediante las vigilancias en contextos digitales. Así, las medidas de vigilancia deben ser legales, tanto en su sentido formal y material, además de ser necesarias y proporcionales.[14]

La legalidad supone que las medidas de vigilancia de los Estados deben estipularse de forma previa a la actuación estatal. Sumado a ello, debe contener "de manera expresa, taxativa, precisa y clara en una ley, tanto en el sentido formal como material"[15] las disposiciones que habiliten la vigilancia. Tal como lo señalan los organismos de Naciones Unidas,

---

7 Corte IDH, Caso de las Masacres de Ituango vs. Colombia. Excepción preliminar, fondo, reparaciones y costas. Sentencia de 1 de julio de 2006. Serie C Nº 148, párr. 193 y 194.

8 Corte IDH. Caso Escué Zapata vs. Colombia. Sentencia de 4 de julio de 2007. Fondo, Reparaciones y Costas. Serie C Nº 165.

9 Corte IDH, Caso Tristán Donoso vs. Panamá. Excepción preliminar, fondo, reparaciones y costas. Sentencia de 27 de enero de 2009. Serie C Nº 193, párr. 55

10 Relatoría Especial para la Libertad de Expresión (2017), "Estándares para una Internet libre, abierta e incluyente", Comisión Interamericana de Derechos Humanos, OEA/Ser.L/V/II CIDH/RELE/INF.17/17. párr. 189

11 Véase Nota N° 5.

12 Naciones Unidas. Ob. cit. párr. 14. En el mismo sentido, RELE, Ob. cit. párr. 212.

13 RELE, Ibídem.

14 Corte IDH. Caso Escher vs. Brasil. Sentencia de 6 de Julio de 2009. Fondo, Reparaciones y Costas. Serie C Nº 200.

15 RELE, Ob. cit. párr. 217

conforme al criterio de legalidad, debe existir como requisito una orden judicial de forma previa a las medidas intrusivas a la privacidad. Lo anterior implica que debe existir un alcance y duración de las medidas de vigilancia, señalando los hechos que justifican las medidas y señalar expresamente los organismos competentes para autorizarlas, implementarlas y supervisarlas.[16] Las facultades de vigilancia deben ser claras, precisas y deben estar detalladas en una ley.[17]

Si bien es cierto que el principio de necesidad no figura de forma explícita dentro del artículo 11 de la CADH, la CIDH ha señalado que para que exista legitimidad en medidas excepcionales que vulneren la privacidad (o intimidad) de las personas deben cumplirse cuatro requisitos: "1) tiene que ser absolutamente necesaria para lograr el objetivo de seguridad en el caso específico; 2) no debe existir alternativa alguna; 3) debería, en principio, ser autorizada por orden judicial; y 4) debe ser realizada únicamente por profesionales de salud".[18] El mismo principio de necesidad puede complementarse a raíz de la construcción doctrinal que ha hecho la misma RELE en cuanto que dicho principio exige que cualquier restricción sea "adecuada y suficientemente justificada".[19]

La proporcionalidad de la medida por tanto "estará dada por el balance entre el objetivo imperioso y necesario, y el impacto de la limitación del derecho individual propuesto".[20] En este sentido, la RELE sugiere que se debe evaluar el impacto que una medida de vigilancia pueda tener en el ejercicio de los derechos humanos en la red, descartando de plano que la vigilancia masiva sea entendida como una medida proporcional.[21] Para el sistema interamericano, situaciones como el terrorismo y la seguridad nacional son coyunturas justificables para establecer medidas de vigilancia, no obstante estas deben ser de forma "limitada y selectiva y de una manera que represente un equilibrio adecuado entre el orden público, las necesidades de seguridad, por un lado, y los derechos a la libertad de expresión y a la privacidad, por el otro".[22]

La CIDH ha señalado que las tareas de vigilancia que "invadan la privacidad de las personas deben ser autorizadas por autoridades judiciales independientes, que deben dar cuenta de las razones por las cuales la medida es idónea para alcanzar los fines que se persigue en el

---

16 CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013. Párr. 74 y 75.

17 En el mismo sentido Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión del Relator Especial de las Naciones Unidas para la protección y promoción del derecho a la libertad de expresión y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. 2013, párr. 8.

18 Véase CIDH, caso "X" y "Y" c. Argentina, párr. 68 (1996), extraído del libro O'Donnell, Daniel. "Derecho internacional de los Derechos Humanos: normativa, jurisprudencia y doctrina de los Sistemas Universal e Interamericano", OACNUDH, México D.F., 2° edición, 2012. p. 572

19 CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013. Párr. 61. En este caso la CIDH se refería a una inspección vaginal realizada en una cárcel en Argentina a la madre y la hija de un recluso que le visitaban.

20 RELE, Ob. cit. párr. 222.

21 Ibidem.

22 Ibid. párr. 223.

caso concreto (…) de si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario; y de si resulta proporcional respecto del interés que se quiere promover".[23] Por lo que una medida de vigilancia intrusiva a la privacidad debe ser justificada previamente por una autoridad judicial, de modo que la medida esté fundada legalmente, sea precisa e indique claramente las reglas que la justifican.[24]

Finalmente, el SIDH ha señalado que las prácticas de vigilancia deben cumplir estándares de transparencia. Es decir, los Estados deben "publicar estadísticas respecto al número de solicitudes realizadas, las aprobadas, las rechazadas, el tipo de investigación en el marco de la cual se solicitan, la duración de dichas medidas, desglose de solicitudes por proveedor, entre otros".[25] Esto dado que un Estado democrático debe dar cuenta de las medidas intrusivas que realiza para con sus ciudadanos. De la misma forma, bajo el amparo del derecho al acceso a la información, las "la vigencia, naturaleza, alcance e implementación de mecanismos de interceptación y monitoreo deben ser públicas y el Estado está obligado a aplicar el principio de máxima divulgación".[26]

3.2. Leyes de inteligencia: organismos de inteligencia y facultades

3.2.1.Argentina

Según el artículo 6° de la Ley 25.520 (actualizada, por la Ley 27.126), el Sistema de Inteligencia Nacional argentino está compuesto por los siguientes organismos: (a) la Secretaría de Inteligencia; (b) la Dirección Nacional de Inteligencia Criminal (dependiente de Secretaría de Seguridad Interior); y (c) la Dirección Nacional de Inteligencia Estratégica Militar (dependiente del Ministerio de Defensa). La misma Ley establece que una Agencia Federal de Inteligencia (en adelante, AFI) será el organismo superior del Sistema de Inteligencia Nacional, dirigiendo y abarcando los organismos señalados, la que dependerá de la Presidencia de la Nación.

De este modo, las funciones de la AFI están señaladas en el artículo 8° de la misma Ley señalando que:

> 1. La producción de inteligencia nacional mediante la obtención, reunión y análisis de la información referida a los hechos, riesgos y conflictos que afecten la defensa nacional y la seguridad interior, a través de los organismos que forman parte del sistema de inteligencia nacional.
> 2. La producción de inteligencia criminal referida a los delitos federales complejos relativos a terrorismo, narcotráfico, tráfico de armas, trata de personas, ciberdelitos, y atentatorios contra el orden económico y financiero, así como los delitos contra los

---

23 CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013. Párr. 165.

24 Corte IDH. Caso Escher vs. Brasil. Sentencia de 6 de Julio de 2009. Fondo, Reparaciones y Costas. Serie C Nº 200. Párr. 131.

25 RELE, Ob. cit. párr. 225

26 Ibid. párr. 217

> poderes públicos y el orden constitucional, con medios propios de obtención y reunión de información."

También cabe señalar que la Ley impide a todos los organismos de inteligencia:

> 1. Realizar tareas represivas, poseer facultades compulsivas, cumplir, por sí, funciones policiales. Tampoco podrán cumplir funciones de investigación criminal, salvo ante requerimiento específico y fundado realizado por autoridad judicial competente en el marco de una causa concreta sometida a su jurisdicción, o que se encuentre, para ello, autorizado por ley, en cuyo caso le serán aplicables las reglas procesales correspondientes.
> 2. Obtener información, producir inteligencia o almacenar datos sobre personas, por el solo hecho de su raza, fe religiosa, acciones privadas, u opinión política, o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción.
> 3. Influir de cualquier modo en la situación institucional, política, militar, policial, social y económica del país, en su política exterior, en la vida interna de los partidos políticos legalmente constituidos, en la opinión pública, en personas, en medios de difusión o en asociaciones o agrupaciones legales de cualquier tipo.
> 4. Revelar o divulgar cualquier tipo de información adquirida en ejercicio de sus funciones relativa a cualquier habitante o a personas jurídicas, ya sean públicas o privadas, salvo que mediare orden o dispensa judicial.

La misma ley regula la interceptación y captación de comunicaciones (art. 18-23 Ley 25.520) señalando expresamente que las comunicaciones privadas "son inviolables en todo el ámbito de la República de Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario" (art. 5° Ley 25.520).

Por otro lado, la ley contempla mecanismos de supervigilancia y fiscalización por parte de una Comisión Bicameral del Congreso (art. 31° Ley 25.520). Se contempla que el Sistema de Inteligencia "se ajuste estrictamente a las normas constitucionales, legales y reglamentarias vigentes, verificando la estricta observancia y respeto de las garantías individuales consagradas en la Constitución Nacional, los Tratados de Derechos Humanos suscriptos" (art. 32° Ley 25.520). De este modo se asegura una mayor transparencia en la utilización de los fondos de carácter reservado (art. 38 bis Ley 25.520).

No obstante lo anterior, organismos de la sociedad civil han resaltado que el Decreto N°656/16 que aprobó un "nuevo" estatuto para la AFI, que derogó un régimen de administración de fondos que distinguía entre fondos públicos y reservados, hizo que en la práctica todo el presupuesto de la AFI terminará como secreto.[27] Sumado a lo anterior, se introdujo nuevamente la "disciplina del secreto" (art. 4 párrafo final, Decreto 656/2016) siendo un "retroceso en una democracia que por primera vez había logrado dar publicidad a información básica sobre la

---

27 ADC & Privacy International, "The state of privacy in Argentina", January 2018. Disponible en: https://privacyinternational.org/state-privacy/57/state-privacy-argentina

organización y el funcionamiento del sistema de inteligencia".[28] Además, se denuncia que todo el personal AFI –con el decreto– pasa a ser "personal de inteligencia", no distinguiendo los casos que fueran realmente necesarios dadas sus funciones y labores a desarrollar. Finalmente, se critica que se derogó la metodología de trabajo de "inteligencia por problemas", que permitía que la producción de material de inteligencia debía ser aprobada por el Director General incluyendo fundamentación, tema específico, duración y ámbito.[29] De esta manera, las funciones y limitaciones señaladas en la Ley se ven mermadas por un decreto (infralegal) carente de principios normativos respetuosos con un Estado democrático de Derecho.

3.2.2.Brasil

La Ley 9.883 de 1999 establece el nuevo Sistema Brasileño de Inteligencia (SISBIN) y crea la Agencia Brasileña de Inteligencia (ABIN), teniendo como objetivo integrar las acciones de planificación y ejecución de las actividades de inteligencia en Brasil. Según el artículo 3° de esta Ley, la ABIN es responsable de "planificar, ejecutar, supervisar y controlar las actividades de inteligencia del país". El SISBIN se encuentra diseminado en 39 órganos repartidos en 20 ministerios, órganos facultados para actuar con el fin de obtener y compartir informaciones estratégicas en el ámbito de su competencia según los planteamientos presidenciales sobre políticas de inteligencia.[30]

A pesar que bajo esta normativa y sus decretos no se consideran expresamente actuaciones de vigilancia o interceptación, el artículo 6°, apartado V, del Decreto 4376/2002 permite a los organismos de este sistema que puedan "intercambiar y brindar la información solicitada para dar conocimiento de las actividades de inteligencia".[31] Se expresa que los organismos del SISBIN "tendrán el derecho a acceder, a través de medios electrónicos, a las bases de datos de sus organismos de origen, sujeto a las normas y límites de cada institución y a las leyes de seguridad, secreto profesional y protección de cuestiones confidenciales".[32] Lo anterior, advierte la sociedad civil, no faculta a la ABIN para "exigir información" a otros organismos del Estado ni empresas de telefonía (tales como metadatos, información de cuentas, registro de comunicaciones (contenido), entre otras.).[33]

El artículo 1° de la Ley 9883/1999 establece que las actuaciones y funciones del SISBIN debe "cumplir y preservar los derechos y garantías individuales y demás dispositivos de la Constitución Federal, los tratados, convenciones, acuerdos y ajustes internacionales en que la República Federativa del Brasil sea parte o signatario, y la legislación ordinaria". Misma

28 ICCSI, "Agencia Federal de Inteligencia: ¿vuelta al oscurantismo?, 1 de junio 2016. Disponible en: http://www.iccsi.com.ar/agencia-federal-de-inteligencia-vuelta-al-oscurantismo/

29 Ibid.

30 Véase página web oficial del Sistema Brasileño de Inteligencia (SISBIN). Disponible en: http://www.abin.gov.br/es/atuacao/sisbin/

31 Antonialli, Dennys y de Souza Abreu, Jacqueline. "Vigilancia estatal de las comunicaciones en Brasil y la protección de los derechos fundamentales", EFF & Internet Lab, Marzo 2016. p. 24

32 Ibidem.

33 Ibid. p. 40-42

fórmula respetuosa de la Constitución y tratados internacionales se establece en el artículo 3° párrafo único. De esta forma, no se configuran expresamente controles judiciales para actuaciones vulneratorias a los derechos humanos, pero la remisión de la norma a la Constitución permite desprender que será necesaria, al menos en el caso de la interceptación de comunicaciones, una autorización judicial, dado lo señalado en el artículo 5° numeral 12° de la Constitución brasileña.

La normativa en comento señala que la ABIN está sujeta tanto a controles internos como externos, siendo las fiscalizaciones de responsabilidad tanto del Poder Ejecutivo como del Legislativo. El control interno se ejerce por la Cámara de Relaciones Exteriores y Defensa Nacional (Creden) del Consejo de Gobierno, que es responsable por definir las directrices de actuación de la ABIN. Las partidas presupuestarias son resguardadas por la Secretaría de Control Interno de la Presidencia de la República (CISET/PR). Los controles externos están llevados por el Poder Legislativo por intermedio de la Comisión Mixta de Control de las Actividades de Inteligencia y el Tribunal de Cuentas de la Unión (TCU).

Dichas Comisiones carecen de facultades investigativas específicas y, en general, poseen facultades muy limitadas, careciendo de acceso a materias clasificadas, facultades de citas compulsivas al personal de inteligencia o acceso a sedes o dependencias de inteligencia,[34] siendo en la práctica poco controladas y fiscalizadas por órganos externos que puedan contrapesar sus autoridades. De esta forma, se ha concluido que tales facultades de control "son insuficientes conforme a estándares internacionales".[35]

3.2.3.Chile

El año 2004, Chile promulga la Ley 19.974 que crea un Sistema de Inteligencia del Estado y una nueva Agencia Nacional de Inteligencia (ANI). El objetivo general del sistema es "proteger la soberanía nacional y preservar el orden constitucional" (art. 4° Ley 19.974). El sistema está integrado por diversos órganos, los cuales son (art. 5° Ley 19.974):

a) La Agencia Nacional de Inteligencia;

b) La Dirección de Inteligencia de Defensa del Estado Mayor de la Defensa Nacional;

c) Las Direcciones de Inteligencia de las Fuerzas Armadas; y,

d) Las Direcciones o Jefaturas de Inteligencia de las Fuerzas de Orden y Seguridad Pública.

La misma ley distingue entre servicios de inteligencia militar y policial, donde los primeros tienen por función detectar, neutralizar y contrarrestar, dentro y fuera del país, las actividades que puedan afectar la defensa nacional y que corresponden a las Fuerzas Armadas y a la Dirección de Inteligencia de Defensa del Estado Mayor de la Defensa Nacional; y los

---

34 Ugarte, José Manuel. "Actividad de inteligencia en América Latina características, fortalezas, debilidades, perspectivas de futuro". Revista Política y Estrategia, Academia Nacional de Estudios Políticos y Estratégicos, N° 127, 2016. p. 62

35 Ibid. p. 59

segundos, "el procesamiento de la información relacionada con las actividades de personas, grupos y organizaciones que de cualquier manera afecten o puedan afectar las condiciones del orden público y de la seguridad pública interior y que corresponden ser ejercidas por Carabineros de Chile y por la Policía de Investigaciones de Chile".[36]

Las funciones de la ANI están detalladas en el artículo 8° de la Ley 19.974, donde destaca principalmente que la Agencia de Inteligencia podrá (entre otras funciones):

> a) Recolectar y procesar información de todos los ámbitos del nivel nacional e internacional, con el fin de producir inteligencia y de efectuar apreciaciones globales y sectoriales, de acuerdo con los requerimientos efectuados por el Presidente de la República.
>
> e) Requerir de los servicios de la Administración del Estado comprendidos en el artículo 1° de la ley Nº 18.575[37] los antecedentes e informes que estime necesarios para el cumplimiento de sus objetivos, como asimismo, de las empresas o instituciones en que el Estado tenga aportes, participación o representación mayoritarios. Los mencionados organismos estarán obligados a suministrar los antecedentes e informes en los mismos términos en que les sean solicitados, a través de la respectiva jefatura superior u órgano de dirección, según corresponda.

Como todas las agencias de inteligencia, la función principal es recolectar y procesar información para cumplir los objetivos de seguridad previstos en la ley. Por regla general, la información que recolecta y procesa la ANI es aquella que está abiertamente disponible, desde fuentes abiertas.[38]

Solamente en casos "estrictamente indispensables para el cumplimiento de los objetivos del Sistema" y cuando la información necesaria "no pueda ser obtenida de fuentes abiertas" (art. 23 Ley 19.974) se podrán conducir procedimientos especiales de obtención de información. El mismo artículo señala que tales procedimientos estarán limitados exclusivamente a "actividades de inteligencia y contrainteligencia que tengan por objetivo resguardar la seguridad nacional y proteger a Chile y su pueblo de las amenazas del terrorismo, el crimen organizado y el narcotráfico" (art. 23 inc. 2° Ley 19.974). Además, si quien busca la realización de estos procedimientos es el Director de la ANI, los procedimientos no son realizados por funcionarios de la ANI (que carece de capacidad operativa directa), sino ejecutados por la Fuerza de Orden y Seguridad que se indique en la resolución judicial que autorice la medida (art. 27 Ley 19.974).

---

36 Rayman, Danny. "Chile: Vigilancia y derecho a la privacidad en internet", Revista chilena de Derecho y Tecnología, Centro de Estudios en derecho informático, Vol. 4, N° 1, 2005. p. 210. Véase además art. Art. 22 Ley N° 19.974.

37 Básicamente todo el aparato de administración estatal: "Ministerios, las Intendencias, las Gobernaciones y los órganos y servicios públicos creados para el cumplimiento de la función administrativa, incluidos la Contraloría General de la República, el Banco Central, las Fuerzas Armadas y las Fuerzas de Orden y Seguridad pública, los Gobiernos Regionales, las Municipalidades y las empresas públicas creadas por ley" (art. 1 inc. 2, 18.575).

38 Concepto de suyo problemático contenido en el artículo 4 de la Ley 19.628 sobre protección de la privacidad, como una excepción a la obligación de recoger el consentimiento para el tratamiento de datos personales, pero que no se define en forma clara en dicho cuerpo legal y ha dado pie a innumerables excesos.

Los procedimientos especiales a que se refiere la ley son los siguientes (art. 24 Ley 19.974):

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

b) La intervención de sistemas y redes informáticos;

c) La escucha y grabación electrónica incluyendo la audiovisual; y,

d) La intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información.

A diferencia de la Ley de Inteligencia brasileña, acá sí se otorgan muy amplias facultades de escuchas e interceptación de comunicaciones para objetivos laxos señalados en la ley. No obstante, la ley igualmente contempla controles de carácter judicial. De este modo, señala la ley, deberá existir "autorización judicial para emplear los procedimientos señalados en las letras a) a d)" (art. 25 Ley 19.974), siendo un Ministro de la Corte de Apelaciones competente quien tendrá que pronunciarse al respecto. La resolución al respecto se dará "sin audiencia ni intervención del afectado ni de terceros, y será fundada" (art. 28), la que debe incluir "la especificación de los medios que se emplearán, la individualización de la o las personas a quienes se aplicará la medida y el plazo por el cual se decreta, que no podrá ser superior a noventa días, prorrogable por una sola vez hasta por igual período" (art. 28 inc. 2° Ley 19.974). Finalmente, cabe destacar que si bien existe la obligación legal de una autorización judicial frente a las cuatro hipótesis señaladas precedentemente, la ley estipula que no será necesaria una autorización judicial para "el uso de informantes, entendiéndose por tales, a las personas que no siendo funcionarios de un organismo de inteligencia, le suministran antecedentes e información para efectuar el proceso de inteligencia" (art. 32 Ley 19.974).

De este modo, a pesar de que la ley contempla autorizaciones judiciales frente a la interceptación de comunicaciones, estas no están orientadas bajo los principios de necesidad, idoneidad y proporcionalidad.[39] Junto con ello, si bien existen controles internos (art. 34 Ley 19.974) y externos (que corresponde a la Contraloría General, tribunales de justicia y la Cámara de Diputados según lo dispuesto en el art. 36) estas solo lo harán en el ámbito de sus competencias, no señalando facultades expresas para las funciones que realiza y no existiendo en la práctica ninguna clase de denuncias frente a posibles abusos.[40]

3.2.4.Colombia

En el caso colombiano, la ley señala que las funciones de inteligencia y contrainteligencia son llevadas a cabo por las Fuerzas Militares, la Policía Nacional, la Unidad de Informa-

39 A pesar que se ha señalado que dentro de la normativa subyacen los principios de necesidad, idoneidad y proporcionalidad. No obstante, acá se establece que si bien podría entenderse como tal, lo anterior no queda claramente explicitado como sí lo hacen otras legislaciones estudiadas. Véase Lara, J. Carlos y Hernández, Valentina. "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Chile", EFF & Derechos Digitales, 2016. p. 28. Disponible en: https://www.eff.org/es/country-reports/Chile-ES-final

40 Ugarte, José Manuel. Ob. cit. p. 63

ción y Análisis Financiero (UIAF), y por los demás organismos que faculte la ley (art. 3 Ley 1621/2013). Las funciones de inteligencia y contrainteligencia están contempladas en el artículo segundo, que ordena "la recolección, procesamiento, análisis y difusión de información, con el objetivo de proteger los derechos humanos, prevenir y combatir amenazas internas o externas contra la vigencia del régimen democrático, el régimen constitucional y legal, la seguridad y la defensa nacional, y cumplir los demás fines enunciados en esta Ley".

Los fines detrás del aparataje estatal para la actuación de recopilación de información de inteligencia y contrainteligencia son los siguientes (art. 4 Ley 1621/2013):

a. Asegurar la consecución de los fines esenciales del Estado, la vigencia del régimen democrático, la integridad territorial, la soberanía, la seguridad y la defensa de la Nación;

b. Proteger las instituciones democráticas de la República, así como los derechos de las personas residentes en Colombia y de los ciudadanos colombianos en todo tiempo y lugar –en particular los derechos a la vida y la integridad personal– frente a amenazas tales como el terrorismo, el crimen organizado, el narcotráfico, el secuestro, el tráfico de armas, municiones, explosivos y otros materiales relacionados, el lavado de activos, y otras amenazas similares; y

c. Proteger los recursos naturales y los intereses económicos de la Nación.

En cuanto a las medidas intrusivas que permite la ley para la satisfacción de sus fines y objetivos, se establece expresamente el "monitoreo del espectro electromagnético e interceptaciones de comunicaciones privadas" (art. 17° Ley 1621/2013). En ella se establece que, por un lado "el monitoreo no constituye una interceptación de comunicaciones" (art. 17° inc. 1) y que "la interceptación de conversaciones privadas telefónicas o fijas, así como las comunicaciones privadas de datos, deberán someterse a los requisitos establecidos en el artículo 15 de la Constitución y el Código de Procedimiento Penal y solo podrán llevarse a cabo en el marco de procedimiento judiciales".

Lo anterior debe leerse a la luz de lo señalado en los artículos 4° y 5° de la Ley 1621/2013. En el artículo 4° se señala que las funciones de inteligencia tendrán como límites el "ejercicio al respeto de los derechos humanos y al cumplimiento estricto de la Constitución, la Ley y el Derecho Internacional Humanitario y el Derecho Internacional de los Derechos Humanos. En especial, (…) por el principio de reserva legal que garantiza la protección de los derechos a la honra, al buen nombre, a la intimidad personal y familiar, y al debido proceso". Sumado a lo anterior, el artículo 5° de la misma Ley señala que quienes autoricen actividades de inteligencia y contrainteligencia deberán observar, además del artículo 4°, los principios de necesidad, idoneidad y proporcionalidad (en forma explícita).

El artículo 15° de la Constitución colombiana protege expresamente el derecho a la intimidad y la inviolabilidad de las comunicaciones privadas, por lo que pueden ser solo interceptados mediante orden judicial. Sin embargo, la declaración legal que establece que el monitoreo no constituye interceptación de comunicaciones hace revertir el espíritu protector. Karisma y Privacy International destacan que el "monitoreo de espectro electromagnético"

no está definido en ninguna parte del ordenamiento jurídico colombiano, por lo que "podría incluir el análisis y monitoreo de e-mails, mensajes de texto y llamadas telefónicas que son llevados por el espectro electromagnético".[41] Por otro lado, a diferencia de otras normativas, existe una mención expresa a los principios de necesidad, idoneidad y proporcionalidad que deben cumplirse tanto por quienes autoricen las actividades de inteligencia (superiores jerárquicos y tribunales de justicia) como por quienes ejecuten dichas actuaciones.

3.2.5.Guatemala

La ley de la Dirección General de Inteligencia Civil (Decreto N° 71-2005) crea la Dirección General de Inteligencia Civil (DIGICI) que depende del Ministerio de Gobernación (art. 1° D-71-2005). Sus funciones están señaladas en el artículo 3° de la ley, el cual enumera un listado no-taxativo (señala: "principales funciones, sin perjuicio de las que le asignen otras leyes") de las cuales destacan:

- Planear, recolectar y obtener información, procesarla, sistematizarla y analizarla, transformándola en inteligencia.
- Obtener, evaluar, interpretar y difundir la inteligencia para proteger del crimen organizado y delincuencia común, los intereses políticos, económicos, sociales, industriales, comerciales, tecnológicos y estratégicos de la República de Guatemala, dentro del área de inteligencia que le corresponde.
- Recabar y centralizar la información proveniente de las dependencias del Ministerio de Gobernación, intercambiando las mismas, según fuere necesario, con otros órganos de inteligencia del Estado.
- Solicitar la colaboración de autoridades, funcionarios y ciudadanos para la obtención de información que coadyuve al cumplimiento de sus fines.

Como ítem especial, las escuchas telefónicas son reguladas en el artículo 4° de la normativa señalada. En ella se establece que "donde existan indicios de actividades del crimen organizado con énfasis en la narcoactividad y la delincuencia común, en las que hubiera peligro para la vida, la integridad física, la libertad y los bienes de personas determinadas, el Ministerio Público puede solicitar como medida de urgencia, la autorización de una Sala de la Corte de Apelaciones para intervenir temporalmente comunicaciones telefónicas y radiofónicas, electrónicas y similares".

Lo anterior da cuenta en primer lugar de que las hipótesis legales para dar pie a una interceptación de comunicación se da bajo "la narcoactividad y la delincuencia común" cuando exista el peligro a la "vida, integridad física, la libertad y los bienes de personas determinadas". Lo anterior deberá ser autorizado judicialmente por la Sala de Corte de Apelaciones. No existe la necesidad de formar un expediente ni proveer justificación en la resolución de autorización. Tampoco se fija un plazo máximo de interceptación.

---

41 Privacy International, Karisma y De Justicia, "The state of Privacy in Colombia", 2018. Disponible en: https://privacyinternational.org/state-privacy/58/state-privacy-colombia

Los controles frente a las actividades estatales están dados por la "sujeción a la Constitución Política de la República y la presente ley" (art. 24° Decreto 71-2005). Sumado a lo anterior, existe un control interno bajo el Viceministro de Gobernación, el cual puede "verificar la planificación, los controles financieros, revisar el avance de la investigación en asuntos internos, como recomendar sanciones disciplinarias o denuncias al Ministerio Público" (art. 25° Decreto 71-2005) además un control externo que será llevado por una Comisión Específica del Congreso de la República (art. 26° Decreto 71-2005).

3.2.6.México

El aparato de inteligencia mexicano está establecido en la Ley de Seguridad Nacional, específicamente se establece en el artículo 18° al Centro de Investigación y Seguridad Nacional (CISN) como el órgano que deberá "operar tareas de inteligencia como parte del sistema de seguridad nacional que contribuyan a preservar la integridad, estabilidad y permanencia del Estado mexicano, a dar sustento a la gobernabilidad y a fortalecer el Estado de Derecho" (art. 19). De esta forma, la información que pueda recolectar el Centro "podrá ser recabada, compilada, procesada y diseminada con fines de Seguridad Nacional por las instancia autorizadas" (art. 30).

Dentro de las atribuciones que puede ejercer, el CISN goza de autonomía técnica para el cumplimiento de sus funciones y "podrán hacer uso de cualquier método de recolección de información" (art.31). Entre ellas, se regula expresamente las intervenciones de comunicaciones (art. 33 a 42) señalando que esta se entiende como "la toma, escucha, monitoreo, grabación o registro, que hace una instancia autorizada, de comunicaciones privadas de cualquier tipo y por cualquier medio, aparato o tecnología" (art. 34 inc. 2). Estas solamente se podrán ejecutar bajo las hipótesis de "amenazas inminentes a la Seguridad Nacional" (art. 5°, 33° y 35°), las cuales son:

a. Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional;

b. Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano;

c. Actos que impidan a las autoridades actuar contra la delincuencia organizada;

d. Actos tendentes a quebrantar la unidad de las partes integrantes de la Federación, señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;

e. Actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada;

f. Actos en contra de la seguridad de la aviación;

g. Actos que atenten en contra del personal diplomático;

h. Todo acto tendente a consumar el tráfico ilegal de materiales nucleares, de armas

químicas, biológicas y convencionales de destrucción masiva;

i. Actos ilícitos en contra de la navegación marítima;

j. Todo acto de financiamiento de acciones y organizaciones terroristas;

k. Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia, y

l. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

Las actuaciones intrusivas de vigilancia deben estar enmarcadas bajo autorización judicial, que en un plazo de 24 horas contadas de la solicitud debe responder mediante una "resolución fundada y motivada" (art. 39), la que puede aplicarse a "comunicaciones y emisiones privadas, realizadas por cualquier medio de transmisión, conocido o por conocerse, o entre presentes, incluyendo la grabación de imágenes privadas". Dicha resolución deberá igualmente fijar un plazo (no mayor a 180 días), los datos de identificación, el tipo de actividad que autoriza y cualquier apreciación que el juez considere necesaria (art. 40). No obstante, en casos de urgencia (art. 49) podrá darse cumplimiento al procedimiento y autorizarse de inmediato si es que esta "compromete el éxito de una investigación y existan indicios de que pueda consumarse una amenaza a la Seguridad Nacional" (art. 49).

Otro control que se señala en la ley es el Control Legislativo. Una Comisión Bicameral, integrada por 3 senadores y 3 diputados (art. 56), podrá solicitar informes del CISN, conocer proyectos e informes, citar al Secretario Técnico para que explique los contenidos de informes generales de las actividades desarrolladas en el semestre anterior. Sumado a ello, la normativa señala que las funciones del Centro deberán preservar los principios de "legalidad, responsabilidad, respeto a los derechos fundamentales y garantías individuales y sociales, confidenciales, lealtad, transparencia, eficiencia, coordinación y cooperación" (art. 61).

Organizaciones de la sociedad civil han señalado que existe una amplia ambigüedad en torno a las circunstancias que justifican las medidas de vigilancia, por lo que las autorizaciones judiciales no bastan para generar contrapesos dentro de la institucionalidad y limitar el poder del Centro. Sumado a lo anterior, no existen salvaguardas tales como "la supervisión de un órgano independiente, obligaciones de transparencia estadística o mecanismos de notificación posterior al afectado por una medida de vigilancia".[42]

Adicional a lo anterior, el artículo 30 de la Ley de Seguridad Interior dictada en 2017 refuerza la posibilidad de que las Fuerzas Federales y las Fuerzas Armadas puedan desarrollar actividades de inteligencia en materia de Seguridad Interior en los ámbitos de sus respectivas competencias. Señalando al efecto que al realizar tareas de inteligencia, las autoridades facultadas por dicha Ley "podrán hacer uso de cualquier método lícito de recolección de in-

---

42 García, Luis Fernando. "Vigilancia estatal de las comunicaciones y protección de los Derechos Fundamentales en México", EFF & R3D, Agosto 2016. p. 24

formación". Lo anterior ha motivado a organizaciones de derechos humanos a sostener que "la vaguedad y amplitud en la redacción de la Ley de Seguridad Interior abre la puerta para que las Fuerzas Armadas lleven a cabo medidas como la intervención de comunicaciones y la recolección de información privada de cualquier individuo a través de cualquier método, sin que existan límites claros ni se establezcan de manera explícita controles democráticos o mecanismos de rendición de cuentas".[43]

3.3. Interceptación de comunicaciones

3.3.1.Argentina

El único órgano estatal encargado de ejecutar interceptaciones de comunicaciones o captaciones de cualquier tipo es la Dirección de Captación de Comunicaciones del Poder Judicial (DCCPJ) que, como indica su nombre, está en la órbita de la Corte Suprema de Justicia, según lo dispuesto en el decreto 256/2015.

La interceptación de comunicaciones se desarrolla bajo el marco de la Ley de Telecomunicaciones (N° 19.978, art. 45 bis), en cuanto establece que las empresas deberán disponer de sus recursos humanos y tecnológicos para la captación y derivación de las comunicaciones que transmiten. Sumado a lo anterior, la Ley de Inteligencia (N° 25.520, art. 22) establece que las órdenes para la interceptación de comunicaciones deberán ser judiciales. A su vez, la Ley de Tecnologías de la Información y las Comunicaciones (N° 27.078, art. 62 letra i.) señala que los Servicios TIC deberán atender a los requerimientos en materia de defensa nacional y seguridad pública formulados por las autoridades competentes. De esta forma, la interceptación de comunicaciones viene dada por un solo organismo pero que encuentra su funcionamiento y justificación en distintas leyes.

El ex Ministro de la Corte Suprema, Ricardo Lorenzetti, señaló que el objetivo de la DCCPJ era "que [el organismo] se convierta en una oficina con una gran capacidad tecnológica que sirva para interceptar no solo comunicaciones telefónicas, sino también los mensajes que se emiten por aplicaciones como Telegram y WhatsApp".[44] No obstante las pretensiones y su capacidad de vigilancia a las comunicaciones privadas, sus limitaciones las podemos encontrar en diferentes fuentes normativas, todas con un espíritu común: la privacidad es un derecho a proteger, por lo que las autorizaciones para su intromisión deben ser judiciales.

El artículo 13 del Código Procesal Penal argentino señala expresamente que "se debe respetar el derecho a la intimidad y a la privacidad del imputado y de cualquier otra persona, en especial la libertad de conciencia, el domicilio, la correspondencia, los papeles privados y comunicaciones de toda índole. Solo con autorización del juez y de conformidad con las disposiciones de este Código podrán afectarse estos derechos".

---

43 Declaración de Red en Defensa de los Derechos Digitales en: "8 puntos clave de la Ley de Seguridad Interior aprobada por los diputados", Animal Político, 30 de noviembre de 2017, Disponible en: https://www.animalpolitico.com/2017/11/seguridad-interior-ley-puntos-clave/

44 La Nación, "Más oficinas para hacer escuchas", 10 de junio de 2016. Disponible en: https://www.lanacion.com.ar/1907437-mas-oficinas-para-hacer-escuchas%7C

En el mismo tenor, la Ley Argentina Digital (Ley 27.078) señala que existe una inviolabilidad de las comunicaciones que comprende "correos postales, el correo electrónico o cualquier otro mecanismo que induzca al usuario a presumir la privacidad del mismo y de los datos de tráfico asociados a ellos, realizadas a través de redes y servicios de telecomunicaciones". Lo anterior da cuenta de la intención de incorporar nuevas tecnologías de comunicación y también la protección de datos de comunicación o metadatos. En la misma ley, las empresas de telecomunicaciones están obligadas a "garantizar a los usuarios la confidencialidad de los mensajes transmitidos y el secreto de las comunicaciones" (art. 62 letra f.). Finalmente, la Ley de Telecomunicaciones establece la inviolabilidad de la correspondencia de telecomunicaciones (art. 19), señalando que solo una orden escrita de un juez competente podrá disponer su interceptación (art. 18).

3.3.2.Brasil

La interceptación de comunicaciones en Brasil está regulada en la Ley 9296/96 ("Ley de Interceptación Telefónica"[45]), aplicable a las "comunicaciones que transcurren vía tecnologías de información y medios telemáticos" (art. 1 Ley 9296/96). De esta forma, no solo incluye las comunicaciones telefónicas sino también cualquier otro tipo de comunicación (como correos electrónicos).[46] Lo anterior fue corroborado por la Corte Suprema brasileña al desestimar que una interpretación amplia de la norma era de carácter inconstitucional, siendo las razones exclusivamente procesales.[47] El artículo 3° de la Ley 9296/96 establece que la interceptación de comunicaciones debe ser ordenada por un juez, a requerimiento de la autoridad policial (en el marco de una investigación criminal) o representante del Ministerio Público bajo una investigación criminal o instrucción procesal penal.

La misma ley señala en su artículo 2° que la interceptación de comunicaciones no será admitida si es que (I) no existen indicios razonables de autoría o participación de una infracción penal; (II) la prueba pueda efectuarse por otros medios disponibles; y, (III) si la pena investigada es como máxima una pena de detención (*detenção*) que es para delitos menores. Sumado a los salvaguardas ya existentes, la ley también contempla un plazo máximo de 15 días, que podrá ser renovada por igual tiempo una vez comprobada la indispensabilidad del medio de prueba (art. 5). No obstante, Internet Lab y EFF han señalado que la "jurisprudencia imperante" hace posible prorrogar el plazo tanto como se requiera a pesar del tenor literal de la norma.[48]

Otra de las normas que se refiere a la interceptación de las comunicaciones es el artículo 7° del Marco Civil de Internet. En ella se señala expresamente la inviolabilidad de la vida

45 Disponible [en portugués] en: http://www.planalto.gov.br/ccivil_03/leis/L9296.htm

46 Coding Rights & Privacy LatAm, "The state of privacy in Brazil", Privacy International, 2018. Disponible en: https://privacyinternational.org/state-privacy/42/state-privacy-brazil

47 Antonialli, Dennys y de Souza Abreu, Jacqueline. Ob. cit. p. 18-19.

48 Ibid. p. 19

privada y su protección en el marco del acceso a internet. El mismo artículo se señala que la interceptación del flujo de las comunicaciones a través de internet deberán realizarse mediante orden judicial.

Finalmente, se contempla una resolución del Consejo Nacional de Justicia (CNJ), la Resolución n°59/08, que establece el procedimiento para solicitar la interceptación y los estándares para las resoluciones judiciales, considerando reglas tales como notificar a las compañías telefónicas y haciendo responsables a los jueces de proteger la privacidad de la información interceptada. Otra resolución, esta vez del Consejo Nacional del Ministerio Público (CNMP), n°36/09, contiene disposiciones respecto a la forma de solicitud y a la realización de las interceptaciones.[49]

A pesar que a primera vista se ve una legislación sólida a favor de la privacidad, en la práctica, distintas organizaciones han acusado vicios en su aplicación en Brasil, sumado al caso de *Escher et. al vs. Brasil* donde la Corte IDH declaró culpable a Brasil por la interceptación telefónicas indebidas a trabajadores y activistas agrícolas por no cumplir el estándar de legalidad (no hubo fundamentos jurídicos adecuados, fue realizada por una autoridad inapropiada, fuera de una investigación en curso y sin notificación a la Fiscalía General). Existe un alto número de escuchas telefónicas e interceptación de correos electrónicos: el año 2013 se interceptaron en Brasil 21.925 teléfonos y 1563 correos electrónicos.[50] El año 2015, la policía federal de Brasil compró un malware para la vigilancia de las comunicaciones a la empresa Hacking Team;[51] además, han existido campañas de desinformación, phishing y malwares, siendo las principales víctimas opositores políticos de los regímenes de turnos y periodista independientes.[52]

3.3.3.Chile

En Chile, la principal fuente normativa para la interceptación de comunicaciones está contemplada en el Código Procesal Penal (CPP). Dentro de los principios que irradian el proceso penal en Chile está la "autorización judicial previa" (art. 9 CPP) el cual establece que "toda actuación del procedimiento que privare al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o lo restringiere o perturbare, requerirá de autorización judicial previa".

El mismo CPP regula la retención e incautación de correspondencia (art. 218) señalando que puede el Ministerio Público solicitarla al juez, incluso antes que la investigación esté

---

49 Ibid. p. 20

50 Coding Rights & Privacy LatAm. Ob. Cit. Disponible en: https://privacyinternational.org/state-privacy/42/state-privacy-brazil. Los datos son bastantes altos si es que comparamos que para ese año en EE.UU, con una población 316 millones de habitantes, se autorizaron el 2013 solo 3.576 y en Alemania, con una población de 80.65 millones, se emitieron 19.398 órdenes iniciales de interceptación el mismo año. Véase también Antonialli, Dennys y de Souza Abreu, Jacqueline. Ob. cit. p.23.

51 Pérez de Acha, Gisela. "Hacking Team malware para la vigilancia en América Latina", Derechos Digitales, marzo 2016. p. 24 Disponible en: https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

52 Bonifaz, Rafael & Delgado-Ron, Andrés. "Casos verificado de uso ilegítimo de softwares de vigilancia por parte de Gobiernos de América Latina (2015-2016)", Revista PUCE, Número 106. p. 327

formalizada, es decir, antes de la comunicación que el fiscal efectúa al imputado, en presencia de un juez que se desarrolla una investigación en su contra. La correspondencia podrá ser "postal, telegráfica o de otra clase (…)" y se podrá disponer de respaldos de la "correspondencia electrónica", por lo que también podría contemplarse la vigilancia electrónica de e-mails y mensajería instantánea. En el mismo sentido, el artículo 219 CPP señala que podrían obtenerse "copias de las comunicaciones transmitidas o recibidas por ellas".

La interceptación de comunicaciones telefónicas es regulada de una forma más exhaustiva que otras formas de comunicación. Se señala que en la medida que existan:

> "fundadas sospechas, basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión, o que ella preparare actualmente la comisión o participación en un hecho punible que mereciere pena de crimen, y la investigación lo hiciere imprescindible, el juez de garantía, a petición del ministerio público, podrá ordenar la interceptación y grabación de sus comunicaciones telefónicas o de otras formas de telecomunicación" (art. 222 inc.1).

Dicha interceptación no podrá exceder de 60 días, aunque el juez puede prorrogar el plazo por "períodos de hasta igual duración" (art. 222 inc.4); si existen hechos y justificaciones admisibles, es posible que el período de escuchas se alargue significativamente. El mismo artículo establece la obligación de las empresas de telecomunicaciones de mantener un listado actualizado de direcciones IP y registros a disposición del Ministerio Público, y frente a una desactualización, negativa o entorpecimiento a la interceptación o grabación estarán sometidos al delito de desacato.

El artículo 14 de la Ley de Terrorismo (Ley 18.314) también faculta al Ministerio Público a interceptar comunicaciones telefónicas e informáticas previa autorización judicial. El artículo 24 de la ley de Drogas (Ley 20.000) permite, bajo la misma modalidad, "medidas de retención e incautación de correspondencia, obtención de copias de comunicaciones o transmisiones, interceptación de comunicaciones telefónicas y uso de otros medios técnicos". El artículo 33 letra a) de la Ley 19.913 hace aplicable a la investigación de los delitos de lavado de dinero y asociación ilícita para el lavado de dinero, la norma especial del artículo 24 de la Ley de Drogas.

El artículo 369 ter del Código Penal, también permite la utilización de la interceptación y grabación de las telecomunicaciones, conforme al artículo 222 del CPP, cuando existen sospechas fundadas de comisión o preparación de delitos referidos a pornografía y explotación sexual infantil, previstos en los artículos 366 quinquies, 367, 367 ter, 374 bis y ter del Código Penal. Lo mismo respecto del artículo 411 octies, referido a tráfico ilícito de inmigrantes, en los casos en que el delito tenga asignada una pena de crimen.

Como se mencionó previamente el Sistema de Inteligencia del Estado y su Agencia Nacional de Inteligencia permite, bajo la misma hipótesis –autorización judicial previa-, la interceptación de comunicaciones. Finalmente, la interceptación de comunicaciones se puede dar –bajo autorización judicial previa- con el objeto de promover y defender la libre competencia de los mercados.[53]

---

53 Rayman, Danny. Ob. cit. p. 211.

Existen una serie de criterios que permiten a los jueces de garantía discernir cuándo se justifica o no la interceptación de comunicaciones. El problema radica en la falta de transparencia en cómo se aplican, si es que se los aplica. El resultado de lo anterior es que, a pesar de la autorización judicial, que debe otorgarse siempre bajo fundadas sospechas y cuando la medida resulte imprescindible para la investigación, se ha revelado que el número de interceptaciones telefónicas está en las decenas de miles, pero con incertidumbre respecto del total. Las estimaciones varían entre 21.893 interceptaciones reportadas por el Ministerio Público para el año 2016,[54] o 59.380 entre 2014 y 2016;[55] o bien, según el Poder Judicial, 5.992 interceptaciones entre enero de 2015 y mayo de 2016,[56] o 19.940 entre enero de 2014 y marzo de 2018.[57] Lo anterior da cuenta de un uso extensivo de la normativa para la solicitud de autorizaciones, pese a la exigencia de pena de crimen, y una cifra desconocida del total de interceptaciones que se realizan sin contar con las autorizaciones judiciales. En consulta con Derechos Digitales, actores del sistema pusieron bajo cuestionamiento la fiabilidad de las cifras oficiales disponibles.

Una instrucción general emanada del Ministerio Público, mediante el Oficio del Fiscal Nacional Nº 060-2014, referido a los criterios de actuación aplicables a la etapa de investigación en el proceso penal (Instructivo 60-2014), aborda en su acápite 4.2 las reglas específicas que durante la investigación deben ser seguidas por los persecutores penales en materia de interceptación de comunicaciones. El Instructivo 60-2014 resume las diferentes fuentes legales de aplicación de la medida de interceptación y, sorprendentemente, consagra que la medida puede afectar "a quien tiene el carácter de imputado, como también a quienes sirven de intermediarios de las comunicaciones o a quienes facilitan sus medios de comunicación al imputado o sus intermediarios".

Como criterio general de actuación se dispone que, además de cumplirse con las exigencias legales, el fiscal solicitante esté en condiciones de controlar debidamente la ejecución de la medida. Para una acertada decisión respecto de la solicitud de la medida se instruye que el fiscal a cargo de la investigación: (i) solicite informe escrito de la policía que justifique la medida respecto de cada uno de los números que se solicita; (ii) ponderar los antecedentes de la investigación para determinar la pertinencia de la medida; (iii) precisar el alcance de la medida solicitada en la solicitud al juez de garantía, incluyendo el tipo de comunicación que se quiere comprender en la medida; y, (iv) revisar que la resolución judicial concuerde con lo solicitado. Adicionalmente se establece la responsabilidad de los fiscales regionales por la seguridad y respaldo de la información que se recoja.

---

54 Chaparro, Andrea. "Fiscalía pidió 91 mil 'escuchas' telefónicas en los últimos cinco años, a un promedio de 50 diarias". El Mercurio, 7 de enero de 2018, p.C8.

55 A. López , V. Rivera y J. Matus. "La PDI realiza el 86% de las interceptaciones telefónicas en el país". La Tercera, 19 de febrero de 2018, p. 16.

56 Rivera, Víctor. "Tribunales autorizaron 5.992 escuchas telefónicas en todo Chile", La Tercera, 5 de junio de 2016. Disponible en: http://www2.latercera.com/noticia/tribunales-autorizaron-5-992-escuchas-telefonicas-en-todo-chile/

57 Cerca, Tamara. "Tribunales decretan más de 20 medidas intrusivas al día: Interceptaciones telefónicas ocupan casi la mitad de la cifra". EMOL, 25 de julio de 2018. Disponible en: https://www.emol.com/noticias/Nacional/2018/07/25/914480/Tribunales-decretan-mas-de-20-medidas-intrusivas-al-dia-Interceptaciones-telefonicas-ocupan-casi-la-mitad-de-la-cifra.html

Durante el curso de la interceptación telefónica, se instruye a los fiscales a cargo: (i) mantener estricto control de los registros de interceptación, incluyendo un informe escrito de la policía de los resultados de la misma transcurrido la mitad del plazo de su vigencia (incluyendo entrega de todos los registros obtenidos); (ii) solicitar información a la policía sobre la diligencia; (iii) controlar que si en el curso de la diligencia se comienza a registrar comunicaciones con números no cubiertos por la orden, la misma se amplíe oportunamente, si procede; y, (iv) informar a juez de garantía acerca del registro de comunicaciones cubiertas por privilegio de cliente-abogado; (v) la solicitud de prórroga de una medida solo puede ser solicitada cuando la medida haya arrojado alguna utilidad; y, (vi) las fiscalías deben resguardar la reserva del registro de las comunicaciones.

Al término de la interceptación, de acuerdo al Instructivo 60-2014, los fiscales deberán: (i) llevar un registro de todas las personas que hayan tenido acceso a las comunicaciones; (ii) requerir a la policía un informe completo que incluya un análisis investigativo; (iii) solicitar al juez de garantía la notificación a los sujetos a cuyos números afectó la medida (salvo riesgo para la integridad física o la vida); y, (iv) solicitar audiencia al juez de garantía para entrega de los registros o destrucción de los mismos.

Como se aprecia, el Instructivo 60-2014 realiza interpretaciones de la normativa legal que no necesariamente se encuentran alineadas con el adecuado balance de la protección de la privacidad. En otros casos, aunque el intento de autoregulación avanza en la dirección correcta de control del ejercicio de las medidas intrusivas, no provee garantía suficiente de que aquellos controles se adopten en la práctica, ni un sistema claro para asegurar su exigibilidad por otros actores del sistema.

3.3.4. Colombia

Tanto en la Constitución (art. 15) como en el Código de Procedimiento Penal (art. 14) se resguarda la privacidad en las comunicaciones privadas, siendo solo posibles de interceptar mediante orden judicial. En el mismo tenor, el artículo 250 de la Constitución señala que debe la Fiscalía General de la Nación "solicitar al juez que ejerza las funciones de control de garantías". Sin embargo, la Constitución permite en el numeral 2 del artículo 240 "adelantar registros, allanamientos, incautaciones e interpretaciones de comunicaciones" donde el juez deberá ejercer el control de garantías en un examen posterior "a más tardar dentro de las treinta y seis (36) horas". Por tanto, en Colombia el control judicial de las intervenciones en las comunicaciones se admite *a posteriori*.

Por otro lado, el Código de Procedimiento Penal regula la retención de correspondencia y su examen, no dando cuenta de la necesidad de una autorización judicial en el mismo momento. En el caso de la retención de correspondencia, lo podrá ordenar el Fiscal General, incluyendo la "correspondencia privada, postal, telegráfica o de mensajería especializada o similar que reciba o remita el indiciado o imputado, cuando tenga motivos razonables fundados" (art. 233 CPP). De la misma forma, la policía judicial "examinará correspondencia retenida" (art. 234 CPP) informando en un máximo de 12 horas al fiscal que expidió la orden.

En caso de la interceptación de las comunicaciones telefónicas y similares (art. 235 CPP) se sigue la misma directriz constitucional de la autorización judicial *a posteriori*. El fiscal puede ordenar la interceptación y grabación de comunicaciones "telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético" cuyas entidades encargadas de la operación técnicas tienen la obligación de realizarla inmediatamente después de la notificación de la orden. Esta tiene una vigencia máxima de tres meses prorrogable "hasta por otro tanto" si es que subsisten motivos fundados que la originaron. De la misma forma se aplica para las "navegaciones por internet y otros medios tecnológicos que produzcan efectos equivalentes" (art. 236 CPP).

La audiencia de control de legalidad posterior (art. 237 CPP), deberá ser en un máximo de 24 horas siguientes al cumplimiento de la retención de correspondencia, interceptación de comunicaciones o recuperación de información dejada al navegar por internet o medios similares.

Dentro de los controles, se ha criticado la ambigüedad del Código a la expresión "las autoridades competentes", quienes son las encargadas de la operación técnica de la interceptación y procesamiento de las comunicaciones.[58] No obstante, la Corte Constitucional ha avalado dicha nomenclatura debido que en su criterio, dado un examen sistémico a la normativa, esta recaería en la policía judicial (tanto el Cuerpo Técnico de Investigaciones como la Policía Nacional).[59]

Finalmente, tenemos la Ley de inteligencia colombiana, que reglamenta la interceptación de las comunicaciones. Su análisis sigue al CPP y la Constitución, cuestión ya analizada en el acápite sobre Ley de Inteligencia colombiana.

3.3.5.Guatemala

La normativa que regula la interceptación de las comunicaciones en Guatemala tiene como principio el texto constitucional que "garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna" (art. 24 Constitución guatemalteca). De este modo, "solo podrán revisarse o incautarse, en virtud de una resolución firme dictada por juez competente".

Guatemala contempla en su Código Procesal Penal una de las fuentes normativas que permite la interceptación de las comunicaciones. Ella supone, en primer lugar, que se podrá interceptar y secuestrar correspondencia "postal, telegráfica o teletipográfica" ante una orden judicial cuya decisión deberá ser fundada y firme" (art. 203 CPP). El juez será el encargado de abrir la correspondencia y revisar si es pertinente o no para la investigación (art. 204 CPP). La misma lógica se aplicará en el caso del control y grabación de las comunicaciones "telefónicas o similares" (art. 205 CPP): el juez será el encargado de revisar el contenido de la interceptación y determinará la pertinencia para la investigación; en caso que no lo sea

---

58 Rodríguez, Katitza y Rivera, Juan Camilo. "Vigilancia de las comunicaciones por la autoridad y protección de los derechos fundamentales en Colombia", EFF, 2015. p. 16. Disponible en: https://www.eff.org/files/2015/05/21/vigilancia_de_comunicaciones_colombia_eff.pdf

59 Ibidem.

ordenará la destrucción de toda grabación o material que no tenga relación, previa noticia al Ministerio Público, al imputado y su defensor.

Otra fuente normativa para la interceptación de las comunicaciones se encuentra estipulada en la Ley contra la delincuencia organizada (Decreto 21-2006). La normativa establece un capítulo especial para la "interceptaciones telefónicas y otros medios de comunicación", siendo esta posible en la medida que sea necesaria para "evitar interrumpir o investigar la comisión de delitos en los artículos 2,[60] 3,[61] 4,[62] 5,[63] 6,[64] 7,[65] 8,[66] 9,[67] 10[68] y 11[69] de la presente ley". Se hace presente que la norma en cuestión tiene una amplia idea de lo entendido por "comunicaciones", comprendiendo "comunicaciones orales, escritas, telefónicas, radiotelefónicas, informáticas y similares que utilicen el espectro electromagnético, así como cualesquiera de otra naturaleza que en el futuro existan" (art. 48, D. 21-2006). Para ello será necesaria una autorización judicial previa solicitud exclusiva del Ministerio Público (art. 49, D. 21-2006) y deberán cumplirse una serie de requisitos para que tenga éxito la solicitud del Ministerio Público (art. 50, D.21-2006), siendo estos:

a. Descripción del hecho que se investiga, indicando el o los delitos en que se encuadran los mismos.
b. Números de teléfonos, frecuencias, direcciones electrónicas, según corresponda, o cualesquiera otros datos que sean útiles para determinar el medio electrónico o informático que se pretende interceptar para la escucha, grabación o reproducción de la comunicación respectiva.
c. Descripción de las diligencias y medios de investigación que hasta el momento se hayan realizado.
d. Justificación del uso de esta medida, fundamentando su necesidad e idoneidad.
e. Si se tuvieren, nombres y otros datos que permitan identificar a la persona o personas que serán afectadas con la medida.

Cabe destacar que la normativa contempla expresamente estándares de "necesidad

---

60 Delito de "Grupo delictivo organizado u organización criminal".

61 Delito de "Conspiración".

62 Delito de "Asociación ilícita"

63 Delito de "Asociación ilegal de gente armada".

64 Delito de "Entrenamiento para actividades ilícitas".

65 Delito de "Uso ilegal de uniformes o insignias".

66 Delito de "Comercialización de vehículos y similares robados en el extranjero o en el territorio nacional"

67 Delito de "Obstrucción a la justicia".

68 Delito de "Exacciones intimidatorias".

69 Delito de "Obstrucción extorsiva de tránsito".

e idoneidad de la medida" (art. 51, D. 21-2006). De esta forma, la autorización de la interceptación de las comunicaciones deberá contemplar los siguientes requisitos para que esta sea conforme a derecho (art. 53, D. 21-2006):

"a. Justificación del uso de esta medida indicando los motivos por los que autoriza o deniega la solicitud de interceptación.

b. Definición del hecho que se investiga o se pretende evitar o interrumpir, indicando el o los delitos en que se encuadran los mismos.

c. Números de teléfonos, frecuencias, direcciones electrónicas, según corresponda, o cualesquiera otros datos que sean útiles para determinar el medio electrónico o informático que se autoriza interceptar.

d. Plazo por el que autoriza la interceptación. La autorización tendrá una duración máxima de treinta días, la cual podrá prorrogarse de conformidad con la presente Ley.

e. Nombres y otros datos que permitan identificar a la persona o personas que serán afectadas con la medida, en caso éstos hayan sido proporcionados por el órgano requirente.

f. La fecha y hora para la audiencia de revisión del informe al que se refiere el artículo 59 de la presente Ley".

A diferencia de la normativa colombiana, la competencia para las interceptaciones quedarán exclusivamente a la Policía Nacional Civil, "quienes serán periódicamente evaluados con métodos científicos para garantizar su idoneidad en el ejercicio de dichas actividades" (art. 55 D. 21-2006). Sumado al resguardo y control de la Policía, es interesante observar que la misma ley contempla un control judicial a las interceptaciones donde deberán "verificar que los procedimientos se estén desarrollando de conformidad a la presente Ley", la que deberá ser realizada personalmente al menos una vez dentro de período autorizado (art. 57 D. 21-2006). También se observa que deberán existir informes del fiscal para el juez cada quince días sobre el desarrollo de la actividad de la interceptación, grabación y reproducción de las comunicaciones (art. 59 D.21-2006).

A pesar que la Ley General de Telecomunicaciones no se regula nada al respecto, se puede señalar que las normativas expuestas hasta aquí (incluida la de Dirección General de Inteligencia Civil) "la empresas de telecomunicaciones están obligadas a colaborar con la interceptación de comunicaciones".[70] La no mención sobre estos temas presenta un desalineamiento respecto de las normativas hasta ahora vistas, no considerando deberes de confidencialidad o protección contra terceros a los datos y metadatos tratados a propósito de la interceptación de comunicaciones.

Dicho lo anterior, se observa una normativa que recoge principios internacionales de derechos humanos en cuanto a la idoneidad y necesidad de la interceptación de las medidas. Además se señala una interesante fórmula, no vista hasta aquí, que es el juez quién revisa

---

70 Fundación Acceso, "¿Privacidad digital para defensores y defensoras de derechos humanos?", San José, Costa Rica, 2015. p. 148

el material obtenido de las interceptaciones de comunicaciones y el secuestro de la correspondencia. Sumado a lo anterior, la autorización judicial se realiza *a priori* con controles *a posteriori* sobre su idoneidad y necesidad, además de una supervigilancia de las actuaciones policiales y del Ministerio Público. No obstante, en entrevista con la activista guatemalteca, Sara Fratti, esta señala que el aparataje estatal provenientes de la dictadura y gobiernos de facto hacen que exista "un aparato estatal ya montado" de interceptación de comunicaciones por parte de la policía y militares tanto a "jueces, periodistas y activistas" del país.[71] La misma opinión se desprende de informes centroamericanos señalando que "las escuchas telefónicas en Guatemala son una práctica reiterada desde hace más de 35 años. La práctica ilegal de las escuchas telefónicas son controladas desde la oficina de control de inteligencia militar".[72] De este modo, la realidad guatemalteca desborda la normativa respetuosa con los derechos humanos.

3.3.6.México

La protección a la inviolabilidad de las comunicaciones se encuentra recogida en el texto constitucional (art. 16 inc. 12 y 13) estableciendo una sanción penal para quien atente contra la libertad y privacidad de las mismas. Solo un juez federal –a petición de una autoridad federal competente o del Ministerio Público- podrá autorizar una intervención de comunicaciones privadas.

El Código nacional de procedimientos penales establece que la intervención de comunicaciones privadas "abarcan todo el sistema de comunicación o programas que sean resultado 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, las cuales pueden presentar en tiempo real" (art. 291 CNPP). Lo anterior da cuenta de una descripción sumamente detallada, en comparación con las normativas revisadas hasta aquí, contemplando mecanismos como e-mails, Whatsapp, Telegram y otros dispositivos de tecnologías. Se descarta, eso sí, que se pueda utilizar para materias no penales (art. 294 CNPP).

Como la misma Constitución señala, las solicitudes del Ministerio Público deben realizarse mediante una autorización judicial para interceptar comunicaciones. Los requisitos de la solicitud del Ministerio Público deberán ser fundados y motivados indicando "el tipo de comunicación a ser intervenida; su duración; proceso que se llevará a cabo y las líneas; número o aparatos que serán intervenidos, y en su caso la denominación de la empresa concesionada del servicio de telecomunicaciones a través del cual se realiza la comunicación objeto de la intervención" (art. 292 inc.1 CNPP). El plazo será de 6 meses, no prorrogable salvo que se acrediten nuevos elementos que lo justifiquen.

De esta forma, el contenido de la resolución judicial que autoriza dicha intervención judicial deberá determinar "las características de la intervención, sus modalidades, límites y en su

---

71 Entrevista personal a Sara Fratti (IPANDETEC), realizada 5 de junio de 2018.

72 Fundación Acceso, Ob. cit. p. 148

caso, ordenará a instituciones públicas o privadas modos específicos de colaboración" (art. 293 CNPP). Finalmente, a diferencia de la norma guatemalteca, los organismos competentes para la intervención de comunicaciones "deberán colaborar eficientemente con la autoridad competente para el desahogo de dicho actos de investigación" (art. 301 CNPP).

La Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro (art. 14 a 17) y la Ley contra la Delincuencia Organizada (art. 15 al 28) regulan en términos casi idénticos al CNPP la intervención de comunicaciones privadas para la investigación de algunos delitos en específico. Del mismo modo, la Ley de Policía Federal regula la intervención de las comunicaciones: "los artículos 16 y 21 de la Constitución Política de los Estados Unidos Mexicanos, Ley Federal Contra la Delincuencia Organizada, Ley de Seguridad Nacional, Código Federal de Procedimientos Penales" (art. 48 Ley de la Policía Federal). Finalmente, debe entenderse como parte del andamiaje normativo mexicano para interceptar comunicaciones lo ya señalado en la Ley de Seguridad Nacional.

Al igual que los demás países analizados, la normativa constitucional no va de la mano de las prácticas de las autoridades estatales mexicanas para la interceptación de comunicaciones. Se ha revelado la utilización del *malware* "Pegasus", del grupo israelí NSO Group, para la intervención de comunicaciones de defensores de derechos humanos, periodistas, activistas y disidentes políticos.[73] Sumado a ello, las denuncias de espionaje a periodistas , activistas y opositores políticos han sido en contra de autoridades políticas que no tienen las facultades legales para realizar interceptación de comunicaciones: "las únicas autoridades facultadas son la Procuraduría General de la República, las Procuradurías Estatales, la Policía Federal y el CISEN".[74] No obstante, se ha acreditado que el software de Hacking Team ha sido adquirido por Secretarías de Gobierno en estados como Jalisco, Querétaro, Puebla, Campeche y Yucatán, además de la empresa de Estado de Petróleos Mexicanos.[75] De esta forma, nuevamente la realidad desborda la normativa constitucional y legal impidiendo un resguardo adecuado de la privacidad en las comunicaciones en México.

3.4. Retención de datos y metadatos por ISPs

3.4.1.Argentina

Para el análisis sobre la normativa en la retención de datos en Argentina se puede partir con el caso Halabi v. PEN (2009). Ahí se estableció que los datos de comunicación (metadatos), para que puedan ser adquiridos por el Ministerio Público y el Poder Judicial, deben seguir la mismas restricciones que existen en la interceptación del contenido de las comunicaciones.[76]

---

73 Perlroth, Nicole. (19 de junio, 2017) "Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families. The New York Times". Disponible en: https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html. Un completo informe sobre la utilización del malware Pegasus puede verse en R3D, Article 19 y Social TIC (2017), "Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México". Disponible en: https://r3d.mx/gobiernoespia/.

74 Pérez de Archa, Gisela. Ob. cit. p. 55

75 Ibidem.

76 ADC & Privacy International. Ob. Cit. Disponible en: https://privacyinternational.org/state-privacy/57/state-privacy-argentina

De este modo, la interpretación que realizó en su momento la Corte Suprema argentina contiene la misma lógica presentada en la sentencia *Escher v. Brasil* sobre la retención de datos de comunicación, lo que es recogido en el artículo 236 del Código de Procedimiento Penal.

A pesar de lo anterior, las empresas prestadoras de telecomunicaciones no tienen la obligación legal a la conservación de datos de tráfico, no obstante "se les permite hacerlo y podrían haberlo hecho en el pasado".[77] Aun así, podemos encontrar en el Reglamento de Calidad de los Servicios de Telecomunicaciones en su artículo 8° que "los prestadores de telecomunicaciones deberán conservar, en archivos electrónicos y por un plazo mínimo de tres años, los datos recogidos, por sus sistemas que sirvieran de base para el cálculo de los indicadores de calidad establecidos por esta normativa". Las autoridades, continúa la norma, podrán requerir la entrega total o parcial de los mismos y proceder a su almacenamiento durante el lapso que considere conveniente. Lo anterior, ha sido catalogada como "discrecional" y posiblemente "contrario a estándares internacional",[78] sobretodo entendiendo que si los metadatos pueden revelar aspectos altamente sensibles, su tratamiento debe regirse por los principios de finalidad y temporalidad de los datos personales.

Finalmente, cabe señalar la Ley 25.891 que establece un Registro de usuarios de teléfonos "con el objetivo de detectar actividades ilícitas realizadas a través de estos dispositivos".[79] La normativa crea una base de datos para registrar teléfonos móviles perdidos o robados, a los que el Estado puede acceder de forma inmediata y a toda hora ante requerimiento del Poder judicial o Ministerio Público.[80] La normativa no establece una definición sobre qué datos pueden ser solicitados, pero obliga a las prestadoras de servicios comunicaciones móviles de informar y compartir "toda la información sobre clientes y usuarios" (art. 8, Ley 25.891), algo totalmente vulneratorio dado que no "se establece un plazo máximo de retención de datos personales ni prohíbe a los prestadores la transferencia de los mismos o un uso distinto".[81]

3.4.2.Brasil

En Brasil, tanto los proveedores de servicios de telefonía fija como los de servicios móviles están obligados a mantener y retener todos los datos relacionados con la provisión de servicios. Por un lado, la Resolução n°426/05 (Normativa del Servicios de Telefonía Fija Conmutada) señala que tales datos deben ser almacenados por al menos cinco años sin que se precise qué datos están incluidos, por quién pueden ser utilizados ni con qué propósitos.[82]

---

77 Ibid.

78 Ferrari, Verónica y Schnidrig, Daniela. "Vigilancia estatal de las comunicaciones y protección de los derechos fundamentales en Argentina", EFF y CELE, Agosto 2016. p. 16

79 Ibid. p. 15

80 Ibidem.

81 Ibidem.

82 Antonialli, Dennys y de Souza Abreu, Jacqueline. Ob. cit. p. 9

Por otro lado, la normativa de Servicios Móviles Personales establece la retención de "documentos de facturación (documentos de naturaleza fiscal), que contengan datos sobre llamadas entrantes y salientes, fecha, hora, duración y precio, así como la información de cuenta de los subscriptores" (art. 10, Resolução n°477/07) por un período mínimo de 5 años.

Finalmente, también la Normativa de Servicio de Comunicación Multimedia (Resolução n°614/13) establece que los proveedores de internet retengan los registros de conexión y datos de cuenta de los suscriptores por al menos un año (art. 53), lo que considera "la fecha y hora del uso de una conexión a internet, una dirección IP específica en la terminal de paquetes de datos entrantes y salientes".[83] De esta forma, los datos y metadatos de telefonía se conservarán por un período de 5 años, mientras que los de internet por el plazo de uno.

Tales normativas deben ser vistas a la luz de las facultades que otorga la Ley de organizaciones criminales (Ley 12.850/13).[84] En concordancia con lo ya señalado, el artículo 17° establece que las "concesionarias de telefonía fija o móvil mantendrá, por un plazo de 5 años, a disposición de las autoridades mencionadas en el artículo 15°, registros de identificación de número de terminales entrantes y salientes de llamadas internacionales, de larga distancia o locales". La obligación, se ha mencionado, no contiene "ninguna disposición que restrinja el uso de los datos retenidos para la investigación"[85] ni tampoco especificaciones sobre qué datos registrar, a qué entidades se le aplica, las limitaciones a accesos ni condiciones de uso y seguridad.[86]

Más preocupante aún es lo estipulado en el artículo 15° en cuanto "el jefe de la policía civil y la Fiscalía General tendrán acceso, sin necesidad de que medie una orden judicial, solamente a la información de cuenta de la persona acusada que indique aptitudes personales, sus padres y la dirección retenida por las Cortes Electorales, empresas telefónica, instituciones financieras, proveedoras de internet y administradores de tarjetas de créditos".[87] Lo anterior permite el acceso a datos personales sensibles sin ninguna clase restricción judicial, como tampoco ninguna clase de justificación en torno a su propósito. De esta manera, "los jefes de policía civil, han solicitado registros telefónicos a las compañías de telefonía sin órdenes judiciales".[88] La normativa anterior se encuentra en una acción directa de inconstitucionalidad pendiente.[89]

---

83 Ibid. p. 10

84 Disponible en portugués en el siguiente link: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm

85 Antonialli, Dennys y de Souza Abreu, Jacqueline. Ob. cit. p. 12

86 Ibidem.

87 Se aplica misma normativa en el artículo 17-B de la Ley de crímenes de Lavado de Dinero (Ley n°9613/99).

88 Antonialli, Denny y de Souza Abreu, Jacqueline. Ob. cit. p. 14

89 El seguimiento se puede realizar en el siguiente link: http://www.stf.jus.br/portal/processo/verProcessoAndamento.asp?numero=5063&classe=ADI&codigoClasse=0&origem=JUR&recurso=0&tipoJulgamento=M

El marco civil de Internet (*Marco civil da Internet*) establece en su artículo 13° que las proveedoras de internet "tiene[n] el deber de almacenar los registros de conexión, en confidencialidad y en un ambiente seguro y controlado, por el período de un año, conforme a la normativa vigente". Tales registros de conexión son "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 dato" (art. 5). A los proveedores de aplicaciones de internet también se les aplica una obligación de retención de data y metadatos, bajo los principios de confidencialidad y seguridad por un rango máximo de seis meses (art. 15).

No obstante lo visto en la Ley de la Policía Federal, para obtener registros de conexión o registros de acceso a aplicaciones de internet es necesario que sea bajo el contexto de un proceso judicial civil o penal, donde el juez lo autorice bajo los criterios de (art. 22):

I. indicios fundados de la ocurrencia del ilícito;

II. justificación motivada de la utilidad de los registros solicitados para fines de investigación o instrucción probatoria; y

III. período al que se refieren los registros.

Para las organizaciones de la sociedad civil debería existir una "declaración de derechos en las comunicaciones telefónicas" que limite la vigilancia en conformidad a los principios internacionales de derechos humanos.[90]

3.3.3.Chile

La normativa chilena sobre retención de datos está en el artículo 222 del Código Procesal Penal y en el Reglamento sobre interceptaciones y grabación de comunicaciones telefónicas y de otras formas de telecomunicación (Decreto 142-2005). En estas se establece que los proveedores de servicios de telecomunicaciones "deberán ... mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, por un período mínimo de un año, de los números IP de las conexiones que realicen sus abonados" (art. 222, Código Procesal Penal). No existe mención de un tiempo máximo de retención, ni se hace explícito el requisito de una orden judicial para su entrega.

El año 2017 se intentó llevar adelante un decreto infralegal para modificar dichas normas y que las compañías de telecomunicaciones pudieran ampliar el registro a "todo tipo de comunicaciones", por un período de dos años. Los datos que se buscaba que retuvieran las empresas, incluían:

- Datos de titular.

---

90 Antonialli, Denny y de Souza Abreu, Jacqueline. Ob. cit. p. 17.

- Llamadas que realiza.
- Con quiénes se comunica.
- Los sitios que visita en internet.
- Tráfico de dato y voz de las comunicaciones.
- Datos de las comunicaciones a través de sistemas de mensajería.
- Ubicación georreferenciada de todos los clientes.

Lo anterior no solamente pretendía modificar la ley mediante un decreto sin discusión en sede legislativa, sino además acumular datos de forma tal que, como se ha señalado, puede vulnerar profundamente la privacidad de las personas, dado que pueden entregar información precisa de las personas, como análisis de patrones de comportamientos, hábitos e incluso predecir comportamientos futuros.[91] La Contraloría General de la República dejó sin efecto dicho decreto, dado que excedía las normas del Código Procesal Penal que se invocaban como fundamento o resultaban aplicables.[92]

3.4.4.Colombia

En Colombia la retención de datos y metadatos puede encontrarse en dos normativas: el Decreto Nº 1704 de 2012, que trata de la retención de datos para efectos de investigación criminal y la Ley Nº 1621 de 2013, que lo hace para efectos de actividades de inteligencia.

El Decreto establece la obligación de los proveedores de redes y servicios de telecomunicaciones de atender oportunamente los requerimientos de interceptación de comunicaciones que efectúe el Fiscal General de la Nación (art. 2°). Los datos que deberán los proveedores suministrar a la Fiscalía General "o demás autoridades competentes", serán los "datos del suscriptor, tales como identidad, dirección de facturación y tipo de conexión", dicha información deberán mantenerla actualizada y conservarla por un término de cinco años (art. 4°). Sumado a ello, deberán los proveedores entregar información específica sobre "sectores, coordenadas geográficas y potencia, entre otras, que contribuya a determinar la ubicación geográfica de los equipos terminales o dispositivos que intervienen en la comunicación" (art. 5°). Finalmente, las actividades deben "garantizar la reserva de los datos y la confidencialidad de la información" (art. 6°).

Lo anterior da cuenta de una poca claridad cuando se refiere a los "proveedores de redes y servicios de comunicaciones", dado que pareciera que los datos que se solicitan son "solo con la telefonía móvil o fija".[93] La misma inquietud surge en cuanto el alcance de lo que a los proveedores se le ordena retener: ¿se limita únicamente a la información de los usuarios o

91 Viollier, Pablo. "Gobierno de Chile busca aumentar su capacidad de vigilancia, aunque sea inconstitucional". Derechos Digitales, 2017. Disponible en: https://www.derechosdigitales.org/11381/gobierno-de-chile-busca-aumentar-su-capacidad-de-vigilancia-aunque-sea-inconstitucional/

92 Véase Cooperativa, "Contraloría dejó sin efecto al "decreto espía" de Aleuy, 28 de noviembre de 2017. Disponible en: https://www.cooperativa.cl/noticias/tecnologia/internet/seguridad/contraloria-dejo-sin-piso-al-decreto-espia-de-aleuy/2017-11-28/154119.html

93 Castañeda, Juan Diego. "¿Es legítima la retención de datos en Colombia", Fundación Karisma, Bogotá, Colombia, 2016. p. 13

también la relacionada al uso que estos hacen con los servicios contratados?[94] Lo anterior se explicaría porque el Decreto 1704/2012 no "menciona de manera taxativa la información de los usuarios que debe ser conservada por las empresas (…) sino se refiere de manera general a información que permite la identificación de los usuarios".[95]

Por su parte, la Ley de inteligencia (Ley 1621/2013) establece que los organismos de inteligencia podrán pedir cooperación de las entidades públicas y privadas para el cumplimiento de los fines de la ley. De esta forma, los operadores de servicios de telecomunicación estarán obligados a entregar "el historial de comunicaciones de los abonados telefónicos vinculados, los datos técnicos de identificación de los suscriptores sobre los que recae la operación, así como la localización de las celdas en que se encuentran las terminales y cualquier otra información que contribuya a su localización" (art. 44 Ley 1621/2013). El mismo artículo señala que los organismos de inteligencia deberán garantizar la seguridad de la información y no podrán solicitar información a un período que no exceda los cinco años.

Nuevamente no queda claro a qué se refiere la normativa por "historial de comunicación". Sumado a lo anterior cabe señalar que en ninguna de las dos normativas se establece una autorización judicial para el acceso a datos de geolocalización, como tampoco frente a controles judiciales posteriores ni en el contexto de investigación criminal ni en el de actividades de inteligencia.[96]

Al igual que en otros países, existe un sistema de registro de teléfonos móviles.[97] Cuando una persona compra un teléfono, debe entregar información personal para que el operador registre, junto con sus datos, un IMEI (número único asignado a cada dispositivo), el número con el que se identifica la suscripción con el operador (IMSI) y el número de la línea (MSISDN). Además de estos números de registro, existen dos bases de datos (negativa y positiva). El problema es que el número IMEI está asociada a una persona, siendo equivalente a su propia identidad. Junto con ello, según la regulación, cualquier autoridad puede acceder a las bases de datos de IMEI. Se ha entendido este sistema como inconstitucional, dado que no comprende el contexto de vigilancia de las comunicaciones, la dimensión de la privacidad que develan los metadatos y la comprensión holística a la inviolabilidad de las comunicaciones que tiene la legislación colombiana.[98]

3.4.5.Guatemala

A diferencia de los otros países estudiados, Guatemala no regula en su Ley General de Tele-

---

94 Rodríguez, Katitza y Rivera, Juan Camilo. Ob. cit. p. 21

95 Ibidem.

96 Ibid. p. 18

97 Art. 106 Ley 1453, Decreto 1633 y Resolución CRC 3128, toda la normativa dictada el año 2011.

98 Véase el análisis completo en Castañeda, Juan Diego. "Un rastreador en tu bolsillo. Análisis del sistema de registro de celulares en Colombia", Fundación Karisma, 2017. Disponible en: https://karisma.org.co/descargar/un-rastreador-en-tu-bolsillo/

comunicaciones la retención de datos y metadatos. No obstante, podemos encontrar una especie de banco de datos en la Ley de Equipos Terminales Móviles (Decreto número 8-2013).

En ella se establece que debe crearse un "registro de los usuarios actuales y futuros de servicios de telecomunicaciones móviles" (art. 1 N° 1, D. 8-2013). Sumado a otros registros que se establecen en la ley, los operadores de servicios de telecomunicación móvil están obligados a "crear y administrar permanentemente un registro de cada uno de sus usuarios del servicios, móvil, tanto en la modalidad de la línea contratada en el plan pospago o tarifario, como de las líneas prepago u otras formas contractuales que en el futuro pudieren crearse" (art 3°, D. 8-2013). La misma obligación de registrarse la tienen todos los usuarios de servicios de telefonía y comunicaciones móviles (Art. 4, D. 8-2013). Dicho registro será mediante una copia de su "documento legal de identificación personal", la que quedará en posesión del vendedor que debe anotar el número de teléfono asociado al documento de identidad (art. 14, D. 8-2013). Lo anterior deberá ser conservado por el vendedor "por un período de tres (3) años" (art. 14, D. 8-2013).

La misma Ley señala que el Ministerio de Gobernación "podrá solicitar a los operadores de telefonía móvil informes acerca de números telefónicos que, de conformidad con sus investigaciones puedan estar generando tráfico de telecomunicaciones desde centros de privación de libertad de cualquier clase. El operador de telefonía móvil deberá indicar en su informe si de conformidad con sus registros el tráfico telefónico de los números que se le indiquen pueda estar siendo generado desde una celda que esté próxima a un centro de privación de libertad de cualquier clase" (art. 17, D-2013). Sumado a lo anterior, el Código Procesal Penal indica que las oficinas de telecomunicaciones "serán agencias de servicios" y estarán obligadas a responder a los consultantes gratuitamente (art. 74 CPP), en caso que así lo requieran las autoridades, infiriéndose que las empresas de telecomunicaciones están obligadas a colaborar con las autoridades competentes.

Finalmente, existe una Base de Datos Negativa (BDN) que registrará todos los móviles que han sido denunciados como robados, hurtados y reportados como extraviados (art. 2 letra b) D. 8-2013) y que la "Superintendencia de telecomunicaciones deberá compartir (…) con los entidades oficiales competentes a nivel regional o internacional".

3.4.6.México

La Ley Federal de Telecomunicaciones y Radiodifusión señala en su artículo 189 que los concesionarios y proveedores de servicios de aplicaciones y contenidos "están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes". Dichas obligaciones se encuentran enumeradas en el artículo 190, que obliga a los concesionarios de telecomunicaciones a "colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil en los términos que establezcan las leyes".

A diferencia de todas las normativas sobre retención de data y metada, la ley mexicana lista los datos que las concesionarias deben conservar y registrar "desde cualquier tipo de línea

que utilice numeración propia o arrendada" (art. 190 párr. II), las cuales son:

a. Nombre, denominación o razón social y domicilio del suscriptor;

b. 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);

c. 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;

d. Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;

e. Además de los datos anteriores, se deberá conservar 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;

f. En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;

g. La ubicación digital del posicionamiento geográfico de las líneas telefónicas; y,

h. La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación.

El plazo que los concesionarios deberán conservar los datos para una consulta en tiempo real a las autoridades competentes será de 12 meses. Concluido ese plazo, deberán los concesionarios conservar dichos datos por doce meses adicionales en sistema de almacenamiento electrónico. Dichos datos no podrán usarse para fines distintos a los previstos en el capítulo de la Ley (art. 190 párr. III). Misma disposición se encuentra también en el artículo 303 del Código Nacional Procesal Penal de México.

Como se observa, en México no se requiere autorización judicial para obtener metadatos y ubicación georreferenciada de los usuarios, no obstante que el 303 del Código Nacional Procesal Penal de México así lo señala en una primera instancia. Sin embargo, en casos excepcionales, "cuando esté en peligro la integridad física o la vida de una persona o se encuentre en riesgo el objeto del delito, así como en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada, el Procurador, o el servidor público en quien se delegue la facultad, bajo su más estricta responsabilidad, ordenará directamente la localización geográfica en tiempo real o la entrega de los datos conservados a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, quienes deberán atenderla de inmediato y con la suficiencia necesaria" (art. 303 inc. 6°). El Mi-

nisterio Público deberá informar la obtención de metadatos y ubicación geográfica al juez de control que deberá ratificar en un plazo de 48 horas después de la medida.

Finalmente, cabe señalar que la Ley General de Transparencia y Acceso a la Información Pública (art. 70 XLVIII) "obliga a las autoridades a publicar el listado de solicitudes que han hecho a concesionarios y proveedores de servicios y aplicaciones de internet respecto a intervención de comunicaciones y registros de datos y geolocalización".[99] México es el único país de los analizados con rendiciones de cuenta y transparencia en materia de interceptación de comunicación y retención de data y metadatos.

3.5. Televigilancia

3.5.1.Argentina

A nivel nacional podemos encontrar la resolución del Ministerio de Seguridad de la Presidencia de la Nación, resolución 238/2012 ("Protocolo General de Funcionamiento de Videocámaras en Espacios Públicos") y la disposición 20/2015 de la Dirección Nacional de protección de datos personales.

La primera normativa establece que la "supervisión, monitoreo y uso de videocámaras de seguridad se limita exclusivamente a las autoridades públicas competentes (…) debiendo garantizar un funcionamiento sustentado en principios de legalidad y respeto de la privacidad de las personas" (N° 2, Protocolo General de Funcionamiento de Videocámaras en Espacios Públicos). Dichas autoridades serán la "Policía Federal Argentina, Gendarmería Nacional, Prefectura Naval Argentina y/o Policía de Seguridad Aeroportuaria" (N° 1, Protocolo General de Funcionamiento de Videocámaras en Espacios Públicos). La finalidad será la prevención del delito y brindar la posibilidad de que se utilicen como prueba documental en procesos judiciales;[100] dado lo anterior, es que deben respetarse las exigencias previstas en la ley de protección de datos (Ley 25.326), señala el N° 14 Protocolo General de Funcionamiento de Videocámaras en Espacios Públicos: "en materia de procedimiento, tratamiento de datos, deber de reserva y *confidencialidad*, protección y resguardo de información, cumplimiento exclusivo de la finalidad específica de su creación, funcionamiento e inscripción de banco de datos exigidos por la Ley". Cabe rescatar que además se prohíbe todo seguimiento, análisis o registros con información motivada con fines discriminatorios (n° 8 Protocolo General de Funcionamiento de Videocámaras en Espacios Públicos).

Por otro lado, la Disposición 20/2015, "Condiciones de Licitud para la Recolección de Datos Personales a través de VANTs o drones" de la Dirección Nacional de Protección de Datos (ahora Agencia de Acceso a la Información Pública), establece que los drones son un "riesgo

---

99 Castañeda, Juan Diego. Ob. cit. p. 19

100 Cejas, Eileen Berenice y González, Carlos César. "Estado de la normativa sobre videovigilancia en Argentina y su relación con la protección de datos personales", 15° Simposio Argentino de Informática y Derecho, 2015. 177. Disponible en: http://sedici.unlp.edu.ar/handle/10915/55549

serio a la privacidad de terceros".[101] De esta forma, para que existan condiciones de licitud para el uso del uso de drones, estos deberán cumplir los principios estipulados en la normativa sobre protección de datos personales, particularmente los principios de consentimiento, respeto de la finalidad, calidad del dato, seguridad y confidencialidad, ejercicio de los derechos del titular del dato, inscripción y manual de tratamiento de datos. Esto dado que la imagen recopilada por drones (y sistemas de vigilancia área) son considerados datos personales sensibles.

Una de las excepciones al consentimiento previo frente a la recopilación de imágenes por parte de los drones se produce "cuando la recolección de los datos la realice el Estado nacional en el ejercicio de sus funciones" (art. 1 letra c., Disposición 20/2015, Anexo I). Lo anterior ha sido entendida como una amenaza porque puede "dar vía libre a la actuación estatal para vigilar y almacenar información sobre las personas".[102] No obstante, dentro de las recomendaciones de la Disposición 20/2015 precisamente se pretende resguardar la privacidad de las personas (recomendación d.), incluso en lugares públicos, además de evitar el uso de estos dispositivos en establecimientos de salud, culto, sindicales, políticos o aquellas donde se puede presumir la preferencia sexual de las personas (recomendación f.) para evitar dar a conocer preferencias sensibles (origen racial, étnico, convicciones religiosas o de culto, etcétera) y protegidas por la normativa argentina en protección de datos.

3.5.2.Brasil

En Brasil podemos encontrar diversa regulación sobre la videovigilancia. La principal, y más importante, corresponde a la Ley 1/2005 que regula "la video vigilancia por las fuerzas de seguridad en lugares públicos de utilización común". No obstante, tangencialmente se aprecia en Brasil que se regula la televigilancia en torno a los servicios de seguridad privada, la vigilancia electrónica en carreteras y relación de sistemas de videovigilancia en taxis.[103]

Para efectos de este acápite se revisará la ley más importante en torno a la videovigilancia, no obstante poder realizar esbozos sobre la normativa ya señalada. Esta ley sistematiza el uso de la videovigilancia para la seguridad pública, regulando la captación y grabación de imágenes y su posterior tratamiento (art. 1, Ley 1/2005). La utilización de las videocámaras está sometida a los objetivos de la ley, los cuales son (art. 2, Ley 1/2005):

a. protección de edificios e instalaciones públicas y de sus accesos;

b. la protección de las instalaciones con interés para la defensa y la seguridad;

---

101 Dirección Nacional de Protección de Datos personales, Disposición 20/2015, "Condiciones de Licitud para la recolección de datos personales a través de VANTs o drones". Anexo II, letra a). Disponible en: http://www.jus.gob.ar/media/2898655/disp_2015_20.pdf

102 ADC, "Alto en el cielo: exploración sobre tecnologías de vigilancia aérea en Argentina", Buenos Aires, 2017. p. 15

103 Véase [en portugués] las diversas regulaciones en extenso en el siguiente link: https://www.cnpd.pt/bin/legis/leis_nacional.htm#Videovigilancia

c. protección de la seguridad de las personas y bienes públicos o privados, y prevención de la práctica de hechos calificados por la ley como delitos, en lugares donde exista un riesgo razonable de su ocurrencia;

d. prevención y represión de infracciones de carreteras;

e. prevención de actos terroristas;

f. protección forestal y detección de incendios forestales.

Los responsables del tratamiento de las imágenes y sonidos son las fuerzas de seguridad de cada jurisdicción donde es captada la imagen; por otro lado, quienes autorizan la instalación de cámaras fijas es el Gobierno "que tutela la fuerza o servicio de seguridad correspondiente" (art. 3 N° 1, Ley 1-2005). Sumado a lo anterior, la medida está precedida con el parecer de la Comisión Nacional de Protección de Datos (*Comissão Nacional de Proteção de Dados*, CNPD) la que podrá formular recomendaciones y dictar medidas se seguridad garantizando el respeto de los derechos y libertades de los titulares de los datos (art. 3 N° 2 y 7, Ley 1-2005).

Lo anterior demuestra que la utilización de cámaras para la vigilancia debe tener un respeto de los datos personales. La misma ley establece principios rectores para la utilización de las cámaras de video y el respeto de los derechos de las personas, entre ellas destacan (art. 7, Ley 1-2005):

- El uso de cámaras de video se rige por el principio de proporcionalidad.
- Se autoriza el uso de cámaras de video cuando dicho medio se muestre concretamente que sea el más adecuado para el mantenimiento de la seguridad y el orden público y para la prevención de la comisión de delitos, teniendo en cuenta las circunstancias concretas del lugar a vigilar.
- En la ponderación, caso por caso, de la finalidad concreta a la que se refiere el sistema, se tienen en cuenta la posibilidad y el grado de afectación de derechos personales mediante la utilización de videocámaras.
- Está expresamente prohibida la instalación de cámaras fijas en áreas que, aunque estén situadas en lugares públicos, sean, por su naturaleza, destinadas a ser utilizadas en resguardo.
- Está prohibida la utilización de cámaras de video cuando la captura de imágenes y de sonidos abarca el interior de una casa o edificio habitado o su dependencia, salvo consentimiento de los propietarios y de quien lo habita legítimamente o autorización judicial.
- Se prohíbe la captura de imágenes y sonidos en los locales previstos en el apartado 1 del artículo 2 [de la ley 1-2005], cuando dicha captura afecte, de forma directa e inmediata, la intimidad de las personas, o resulte en la grabación de conversaciones de naturaleza privada.

Lo anterior da cuenta que existe un resguardo importante a la privacidad de las personas mediante la aplicación del principios de proporcionalidad (*ponderação)* al momento de

instalar cámaras de vigilancia. Sumado a ello, se observa un principio de confidencialidad (*guardar sigilo*) al momento de tener acceso a las cámaras (art. 9 N° 2 ley 1-2005), que podrán los mismos interesados acceder a las grabaciones y solicitar su eliminación (art. 10 N° 1 ley 1-2005), cuando esta no atente contra la defensa del Estado, seguridad pública, amenaza al ejercicio de derechos o cuando perjudique una investigación criminal (art. 10 N° 1 ley 1-2005).

No obstante la aparente razonabilidad de la normativa, en Brasil existe un amplio uso de la televigilancia para resguardar la seguridad urbana. Se ha denunciado el uso de aparatos militares, como drones y globos de vigilancia, para el resguardo de los eventos de la Copa Mundial (2014) y las Olimpiadas (2016), además de un excesivo uso de cámaras de vigilancia en Río de Janeiro.[104] De este modo, pareciera ser que las políticas de seguridad desbordan la normativa del país.

Más recientemente en una medida cautelar adoptada por un tribunal civil de Sao Paulo, se acogió a demanda colectiva conforme a la normativa de derecho del consumo presentada por el Instituto de Defesa do Consumidor (IDEC) en contra de la implementación de un sistema de cámaras con reconocimiento facial para monitorear las emociones de los pasajeros de la línea 4 del metro de esa ciudad.[105] En la decisión cautelar se sostuvo la ilegalidad del sistema por la falta de información a los consumidores acerca de su implementación y la falta de consentimiento de los mismos, destacando el riesgo de discriminación que dicha recolección de datos biométricos implicaba.

3.5.3.Chile

En Chile no existe una regulación sistemática de la televigilancia. No obstante en el ordenamiento jurídico chileno se puede encontrar una regulación sobre las cámaras de videovigilancia del año 1994 que establece un sistema de vigilancia policial por cámaras de televisión.[106]

En el caso del uso de vigilancia de los espacios públicos, su implementación se ha desarrollado básicamente como resultado de la celebración de convenios entre Carabineros de Chile y las Municipalidades, Gobiernos Provinciales o Regionales, para la instalación y empleo de estos sistemas de videovigilancia con fines preventivos, normalmente en el marco de los programas de seguridad comunal establecidos a partir del año 2004.[107]

---

104 Varon, Joana & Felizi, Natasha. "Salí a cazar equipos de vigilancia en los juegos Olímpicos", Coding Rights, 2016. Disponible en: https://chupadados.codingrights.org/es/sai-para-cacar-equipamentos-de-vigilancia-no-rio-olimpico/

105 Altman, Gustavo. "Em liminar, Justiça impede o uso de câmeras de reconhecimento facial no metrô", Jota, 14 de septiembre de 2018, Disponible en: https://www.jota.info/justica/mp-cancele-cameras-metro-14092018

106 Cordero, Luis. "Video-vigilancia e intervención administrativa: las cuestiones de legitimidad", Revista de Derecho Público, Nº 70, 2008. P. 366

107 Palacios, Patricio. "Análisis crítico del régimen jurídico de videovigilancia de las fuerzas de orden y seguridad pública", Tesis para optar al grado de Magíster con mención en Derecho Público, Facultad de derecho, Universidad de Chile, 2007, p.77.

Para estos efectos, los Gobiernos Provinciales o Regionales invocan como título para la celebración de dichos convenios los artículos 2, letra b) y 4, letra a), de la Ley N° 19.175, Orgánica Constitucional sobre Gobierno y Administración Regional, de 2005, que disponen que dentro de las atribuciones que les corresponde a los intendentes y gobernadores, se encuentran las de ejercer las tareas de gobierno interior, especialmente aquellas destinadas a mantener el orden público y la seguridad de sus habitantes y bienes. Por su parte, las Municipalidades citan el artículo 4º, letra j), de la Ley Orgánica Constitucional Nº 19.704, publicada en el Diario Oficial, el 03 de mayo de 2002, que señala que para el cumplimiento de sus funciones las Municipalidades tendrán, entre otras atribuciones esenciales, el apoyo y el fomento de medidas de prevención en materia de seguridad ciudadana y para colaborar en su implementación, sin perjuicio de las funciones que les competen a la fuerza pública para dar eficacia al derecho, garantizar el orden público y la seguridad pública interior.[108]

La Ley del Tránsito (Ley N° 19.676) autoriza la utilización de equipos automáticos para la detección de infracciones o información como medios de prueba; estas solo pueden ser operadas por Carabineros y/o inspectores municipales, reguladas por un reglamento especial realizado por el Ministerio de Transporte, no obstante dicha regulación "adoptará medidas tendientes a asegurar el respeto y protección a la vida privada, tal como la prohibición de que las imágenes permitan individualizar a los ocupantes del vehículo" (art. 4 inciso V, Ley Nº 19.676).

El D.L. 3607 regula el funcionamiento de los vigilantes privados obligando a instituciones como las bancarias, financieras, empresas de valores y/o empresas estratégicas y de servicios de utilidad pública a tener "sistemas de filmación de alta resolución que permita la grabación e imágenes nítidas". Lo anterior es complementado por el artículo 10 del Decreto 222 de 2013, el cual dispone como medida mínima para resguardar la seguridad de la operación de cajeros automáticos que ellos cuenten con un sistema de grabación de imágenes de alta definición, que mediante una cámara externa capte y almacene aquella actividad que se produzca en torno al cajero durante su operación, y que mediante una cámara interna, incorporada al cajero mismo, permita apreciar nítidamente el rostro y demás características físicas de las personas que interactúen con el cajero automático. Las grabaciones deben conectarse en línea con una central de monitoreo, que permita el acceso inmediato a dichas imágenes en el evento de que se active el sistema de alarma. Las imágenes captadas por el sistema de grabación deben ser almacenadas por un plazo mínimo de 45 días.

Finalmente, podemos encontrar en la Ley 19.327 sobre "derechos y deberes en los espectáculos de fútbol" que exige que los organizadores de tales espectáculos dispongan de cámaras de seguridad para "identificar a los asistentes al espectáculo de fútbol profesional, junto con vigilar el perímetro del lugar donde se celebre el mismo. Estas cámaras deberán ser monitoreadas permanentemente por los organizadores durante el desarrollo del espectáculo, debiendo resguardarse sus imágenes por un período mínimo de noventa días, sin perjuicio de lo señalado en el artículo 3º bis" (art. 5° letra g), Ley 19.327).

---

108 bid, p.77-78.

Desde la perspectiva del procedimiento penal, y la posibilidad de utilizar imágenes como medio probatorio, el Instructivo General 60-2014, señala en su apartado 4.4. que cuando los fiscales deban recurrir a este tipo de evidencia deben ponderar si la ejecución de la diligencia lesiona derechos fundamentales. Sin embargo afirma que las filmaciones o fotografías que se efectúen en la vía pública o lugares de libre acceso público no requerirían de autorización judicial. Ya hemos señalado en 3.3.3. nuestros reparos a las interpretaciones que realiza el instructivo, así como su escasa eficacia como mecanismo de control. Por lo demás en sentencia pronunciada por la Corte de Apelaciones de Santiago, y confirmada luego por la Corte Suprema, se reconoció la existencia de una expectativa de privacidad protegida por la garantía constitucional aún en espacios públicos al señalar: "En efecto, razonable es que al acceder a un lugar público cada persona aspire, entre otros aspectos, que sus conversaciones no sean de acceso público, como también que en su desplazamiento no sea objeto de registro personal, o de seguimientos, es decir, que pueda deambular libremente manteniendo su anonimato frente a quienes le rodean, a menos que incurra en conductas ilegales o se vea involucrado en situaciones de emergencia, pues en tales casos, normal es que tales expectativas de privacidad se desvanezcan".[109]

Tal como ha señalado parte de la doctrina, es necesario que exista una regulación que sistematice la videovigilancia en Chile, dado que la captación y grabación de imágenes por medio de cámaras corresponde a un asunto de derechos fundamentales, que vulneran no solo la privacidad de las personas, sino además la libertad de expresión, el derecho a reunión y de libre circulación, por lo que debiera contemplar principios de legalidad, proporcionalidad y necesidad.[110] Sumado a ello, la forma en que ha funcionado hasta ahora la vigilancia mediante cámaras carece de un marco normativo claro y uniforme respetuoso de los derechos humanos. Las múltiples propuestas que pretenden resolver problemas de seguridad social mediante la puesta en marcha de drones o globos de vigilancia, erosionando la privacidad en espacios públicos,[111] deben ser sometidas a un escrutinio y un balance que hoy carecen de un marco legal para su aplicación, pese al mandato constitucional expreso de que la afectación de derechos fundamentales solo puede realizarse por ley.

3.5.4.Colombia

En Colombia tampoco se puede encontrar una regulación integrada y sistemática de la televigilancia. Solo podemos encontrar la Ley 1843 del 2017 que regula los sistemas de detección de infracciones de tránsito y una norma respecto al uso de cámaras de vigilancia por la policía en cuanto estas se integran al sistema de vigilancia. La norma reza (art. 237, Código Nacional de Policía y Convivencia) así:

---

109 Sentencia de la Corte de Apelaciones de Santiago, de 21 de agosto de 2017, Rol Nº 34.360-2017. Disponible en: http://www.pjud.cl/documents/396543/0/DRONES+LAS+CONDES.pdf/bd244e2b-9591-4256-99f8-d4dd3fd617f1, considerando 27º.

110 Leguina Schenone, Iñaki. "Videovigilancia en espacios públicos, respecto del uso de globos de vigilancia y drones. Necesidad de sistematización y regulación legal", 5° Simposio Internacional LAVITS, Santiago de Chile, 29 y 30 de noviembre, 1 de diciembre de 2017. p. 239.

111 Véase Fundación Datos Protegidos, "Drones en Chile: un análisis de los discursos, industria y los derechos humanos", Santiago de Chile, 2017. pp. 19-22.

> "La información, imágenes y datos de cualquier índole captados y/o almacenados por los sistemas de video o los medios tecnológicos que estén ubicados en el espacio público, o en lugares abiertos al público, serán considerados como públicos y de libre acceso, salvo que se trate de información amparada por reserva legal.
>
> "Los sistemas de video y medios tecnológicos, o los que hagan sus veces, de propiedad privada o pública, a excepción de los destinados para la Defensa y Seguridad Nacional, que se encuentren instalados en espacio público, áreas comunes, lugares abiertos al público o que siendo privados trasciendan a lo público, se enlazará de manera permanente o temporal a la red que para tal efecto disponga la Policía Nacional, de acuerdo con la reglamentación que para tal efecto expida el Gobierno nacional".

De este modo, toda la captación y grabación de video que se dé en espacios públicos se pondrá a disposición de la Policía Nacional sin necesidad de orden judicial. No obstante lo anterior, en el caso de "áreas comunes, lugares abiertos al público o que siendo privados trasciendan a lo público, se requerirá para el enlace a que hace referencia el presente artículo, la autorización previa por parte de quien tenga la legitimidad para otorgarla".

A pesar de lo laxo y ambigua de la norma recién descrita, la Superintendencia de Industria y Comercio ha realizado un esfuerzo por entregar directrices dentro de la regulación existente en Colombia. Para ello ha establecido una guía de protección de datos personales en el contexto de sistemas de vigilancia, por lo que la normativa intenta adecuar la realidad de la televigilancia en Colombia a las leyes vigentes en la protección de datos personales. De esta manera, entiende la guía que la recopilación de imágenes de personas es una forma de tratamiento de datos personales por lo que deben observarse "los principios establecidos en dicha norma, esto es, legalidad, finalidad, libertad, calidad o veracidad, seguridad, confidencialidad, acceso y circulación restringida, y transparencia, así como las demás disposiciones contenidas en el Régimen General de Protección de datos personales".[112]

De este modo, no existe una ley que regule de forma comprensiva y sistemática la videovigilancia en Colombia. No obstante, la misma Corte Constitucional colombiana ha señalado que la videovigilancia pueden afectar los derecho a la la libertad de expresión, de manifestación y reunión, así como el derecho a la intimidad y a la protección de la persona 'en su capacidad de decidir cómo presentarse al mundo'".[113] De esta forma, la instalación de cámaras debe revisar si se supera un examen de proporcionalidad dada la restricción de derechos fundamentales que supone tales medidas.[114]

---

112 Superintendencia Industria y Comercio, "Protección de datos personales en sistemas de videovigilancia", Ministerio de Industria y Turismo, 2016, p. 4. Disponible en: http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Guia_Vigilancia_sept16_2016.pdf

113 Corte Constitucional. Sentencia T-407 de 2012. Magistrado Ponente Gabriel Eduardo Mendoza Martelo. Disponible en: http://www.corteconstitucional.gov.co/RELATORIA/2012/T-407-12.htm

114 Fundación Karisma, "Cámaras Indiscretas: análisis fallido del sistema de video-vigilancia inteligente para Transmilenio", Bogotá, Colombia, 2018. p. 30

3.5.5.Guatemala

En Guatemala no existe una normativa especial ni sistemática en torno a la videovigilancia, como tampoco se contempla una protección especial a los datos personales, lo que impide realizar intentos desde la protección de datos personales para su regulación. De esta manera, la única protección al respecto es la Constitución, lo que a todas luces no basta. Se ha detectado que el Estado guatemalteco monitorea a ciudadanos durante protestas y ha ampliado su monitoreo de televigilancia, incluso se ha denunciado que con la colaboración de Estados Unidos se está monitoreando fronteras mediante drones buscando y capturando narcotraficantes.[115]

3.5.6.México

El año 2015, en el Censo Nacional de Gobierno, Seguridad pública y sistema penitenciario, se reportaron que en México existían 25.631 cámaras de vigilancia para el ejercicio de la función pública –más del doble de lo informado el año 2012.[116] En el ámbito municipal mexicano no se tienen datos al respecto, considerando que allí es donde la industria de la vigilancia se ve con mayor capacidad de crecimiento en los próximos años.[117]

De este modo, la regulación que encontramos en México en torno al tema se encuentra dispersa en legislación estatal, sin una norma federal. Los estados de México, Aguascalientes, Colima y la Ciudad de México (ex Distrito Federal) tienen reglas sobre videovigilancia. Para efectos de observar técnicas legislativas, se revisarán algunas regulaciones entorno al tema para dar cuenta de novedades útiles de cara al objetivo de la investigación.

La ley que regula el uso de Tecnología para la Seguridad Pública de la Ciudad de México señala expresamente en su artículo 15 que el uso y tratamiento de la información que se recaben en los sistemas de televigilancia será para "prevención, investigación y persecución del delito, de infracciones administrativas y para servir como evidencia en juicios de cualquier tipo donde se admitan". Sumado a ello, se señala un principio de licitud estipulando que no podrán ser medios de prueba cuando (art. 16):

- "Provenga de la intervención de comunicaciones privadas no autorizadas conforme a la ley;
- "Cuando se clasifique, analice, custodie, difunda o distribuya sin apegarse a la a ley; y
- "Cuando se obtenga del interior de un domicilio o violente el derecho a la vida privada de las personas".

La más interesante normativa la podemos encontrar en el Estado de México, donde se establece un Centro de Control que llevará el control, registro y procesamiento del sistema de

115 Ávila, Renata. "Mapa centroamericano de actores sobre la libertad de internet en Centroamérica", Fundación Ford, 2018. p. 30

116 Arteaga Botello, Nelson. "Regulación de la videovigilancia en México. Gestión de la ciudadanía y acceso a la ciudad", Espiral, Estudios sobre Estado y sociedad, Vol. XXIII, N°66, 2016. p. 199

117 Ibíd. p. 200

videovigilancia (art. 47, Reglamento de la ley que regula el uso de tecnologías de la información y comunicación para la seguridad pública del estado de México). El organismo emitirá dictámenes de viabilidad, autorizará la instalación de cámaras, inspeccionará y supervigilará los servicios de seguridad privada que cuenten con sistemas de videovigilancia (art.48). Sumado a ello, la utilización de videocámaras en este Estado estará sujeta a los principios de proporcionalidad y riesgo razonable, la proporcionalidad será considerada en su doble aspecto de idoneidad y de intervención mínima (art. 56), además, dicho centro de control conservará una copia hasta el plazo de 366 días naturales (art. 57).

Finalmente, en varias legislaciones estaduales, se hace mención a los principios de tratamiento de datos personales para la implementación de mecanismos de tele-vigilancia.[118]

3.6. Biometría

3.6.1.Argentina

La ley de protección de datos personales no contempla los datos biométricos como datos sensibles. No obstante, existe un Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) introducido vía decreto (N° 1766-2011), el cual tiene como objetivo la seguridad y prevención del delito. Es más, dentro de los considerandos del Decreto se señala expresamente que "contribuir a la comprobación idónea y oportuna en materia de identificación de personas y rastros, en procura de optimizar la investigación científica de delitos y el apoyo a la función preventiva de seguridad".[119]

La autoridad de aplicación de dicho Sistema está a cargo del "Ministerio de Seguridad Nacional" (art. 3°, D.1766/11) siendo el administrador la Policía Federal Argentina (Mediante la Superintendencia de Policía Científica). El sistema cuenta con una Unidad de Coordinación y Seguimiento compuesto por la Dirección Nacional de Policía Científica, el Registro Nacional de las Personas, la Dirección Nacional de Migraciones y las áreas de policía científica de la Policía Federal argentina, la Gendarmería Nacional, la Prefectura Naval argentina y la Policía de Seguridad Aeroportuaria (art. 5°, Decreto 1766/11). Como ha advertido la Asociación por los Derechos civiles, la Unidad de Coordinación "no ha sido conformada", por lo que en la práctica, "quien lleva a cabo tal coordinación es la Dirección Nacional de Policía Científica".[120]

Según la regulación, el Registro Nacional de las personas brindará la información necesaria para que "el sistema automatizado de identificación de huellas digitales (AFIS) y de rostros en uso de la Policía Federal Argentina pueda satisfacer los requerimientos de identificación que formulen los usuarios de SIBIOS" (Art. 2° D. 1766/11).

---

118 Ibarra Sáchez, Ernesto. "Seguridad, protección de datos personales y regulación jurídica de la videovigilancia en México". En: Lopez Romero, Lucero (coord.), Jus informa tic's (cap. II), UNAM, México, 2011. p. 266. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/6/2958/17.pdf

119 Decreto N° 1766/11. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/norma.htm

120 ADC, "La Identidad que no podemos cambiar: cómo la biometría afecta nuestros derechos", Abril 2017, p. 18. Disponible en: https://adcdigital.org.ar/2017/04/26/la-identidad-no-podemos-cambiar-biometria-sibios/

El sistema, cuestionado por su capacidad de vulnerar derechos fundamentales, no fue discutido en instancia legislativa.[121] Asimismo, la normativa no exige ningún estándar de seguridad, confidencialidad, finalidad, ni hace expresa la necesidad de cumplir con los demás principios consagrados en la Ley de protección de datos personales argentina, ni se da a los datos biométricos el carácter de datos personales sensibles. Lo que desprotege aún más tales datos ante posibles divulgaciones no autorizadas, transferencias posteriores u otras, a pesar que ha señalado el organismo a cargo que se cumplen con los lineamiento de la Ley 25.326 de Protección de datos personales.[122]

3.6.2.Brasil

En agosto de 2018 se promulgó la Ley General de Protección de Datos Personales (*Lei Geral de Proteção de Dados Pessoais*, LGPDP). Además de exigir por regla general el consentimiento del titular de los datos para el tratamiento de los mismos, clasifica a los datos considerados sensibles. Entre ellos se menciona a los datos corporales, que incluyen a los referidos a la salud, la información genética y los datos biométricos, así como también los datos sexuales.

En mayo de 2017 se aprobó la creación de la Identificación Civil Nacional (ICN, *Identificação Civil Nacional*). Si bien, es el sistema nacional de identificación no busca un sistema de vigilancia y control para efectos de la seguridad ciudadana, la ICN utilizará la base de datos biométricos que contiene la Justicia Electoral. Ello ha sido criticado por organizaciones de la sociedad civil, dado que el sistema fue puesto en marcha antes de la aprobación de una ley de protección de datos personales, sin la exigencia de cumplir con ningún estándar de seguridad ni protección.[123]

Sumado a ello, cabe destacar la 1ey 12.654 que establece una base de datos para personas condenadas por "crímenes atroces". A pesar que la constitucionalidad de la norma se está resolviendo en el Tribunal Supremo de Brasil, existen 8.225 perfiles genéticos, de los cuales 5.925 son de vestigios de escenas de crímenes y 2.299 por condenados e identificados criminalmente.[124]

3.6.3.Chile

Sin perjuicio de cierta normativa específica, no existe una protección explícita a los datos biométricos en la Ley de protección de datos personales, a pesar de que la doctrina ha en-

---

121 Ibid. p. 17

122 Ibid. p. 22

123 Rena, Paulo y Joana Varon (2015). «Brasil anuncia proyecto para identificación única con la biometría. ¿Cómo está el tema en América Latina?». Oficina Antivigilancia. Disponible en: https://antivigilancia.org/es/2015/07/1430/

124 Barbosa, Renan. "Banco de DNA de criminosos cresce 20%, mas medida e questionada no STF", 14 de febrero 2018. Disponible en: https://www.gazetadopovo.com.br/justica/banco-de-dna-de-criminosos-cresce-20-mas-medida-e-questionada-no-stf-50i7pe22l9631v45n4c6xsshr

tendido que estos pueden ser configurados como datos de carácter sensible por la ley.[125] A pesar de lo anterior, se pueden encontrar diversas políticas públicas que utilizan y buscan la recopilación de datos biométricos para diversos fines;[126] la regulación más preocupante, y que llama la atención, es el artículo 11° de la ley 20.931. En ella se estipula que:

> "El Ministerio Público, Carabineros de Chile, la Policía de Investigaciones de Chile, Gendarmería de Chile y el Poder Judicial deberán intercambiar, de conformidad con el artículo 20 de la ley N° 19.628, los datos personales de imputados y condenados, con el objeto de servir de elemento de apoyo a la labor investigativa en las diversas etapas del proceso penal y de colaboración para una eficaz y eficiente toma de decisiones de los tribunales de justicia y de sustento a las políticas de reinserción".

Lo anterior podría considerar datos de carácter biométrico, dado que el Registro Civil chileno cuenta con un sistema de identificación multibiométrico en pasaportes y documentos de identidad, conteniendo en ellos datos biométricos faciales y dactilares.[127] Tales datos podrían ser usados por las policías en "labores investigativas". Dicho Banco de Datos Unificados (BDU) debe ser reglamentado por un decreto supremo, que a la fecha no ha visto la luz,[128] y que será administrado por el Ministerio Público para que los órganos ya señalados puedan utilizarlos en virtud de sus funciones (art. 11 inc. 2°, 20.931).

La ley Nº 19.970 creó el Sistema Nacional de Registros de ADN, que incorpora el registro de datos de ADN de personas involucradas en la investigación y persecución de delitos, es decir, condenados, imputados, víctimas, desaparecidos y sus familiares, y otros registros de evidencias y antecedentes. El Sistema Nacional de Registros de ADN está compuesto por ADN no codificante, que entrega certeza para la identificación de la identidad de un individuo, pero no entrega información acerca de otros factores sensibles como raza o información de salud (carece de información de expresión de genes).

Existen otras iniciativas de implementar reconocimiento facial para disuadir la evasión del pago del transporte público[129] o combatir la violencia en los estadios, obviando que está en juego la privacidad de las personas y, por tanto, siguiendo el principio de legalidad, deberían ser reguladas por ley y no mediante decretos o actos administrativos.

---

125 Garrido, Romina y Becker, Sebastián. "La Biometría en Chile y sus riesgos", Revista Chilena de Derecho y Tecnología, Vol. 6 (1), 2017. pp 73-76.

126 Véase ADC, "Cuantificando identidades en América Latina", Buenos Aires, mayo 2017. pp. 12- 15

127 Uno de los chips que contiene la cédula de identidad es el e-travel que contiene datos biométricos dactilares y faciales (OACI), particularmente los datos de la cédula de identidad son: minucias del dedo principal en formato ANSI, minucias del dedo secundario en formato ANSI, fotografía del titular en color en formato JPEG-2000 y patrón biométrico de reconocimiento facial en formato ANSI, según los parámetros de la Organización de Aviación Civil Internacional (OACI).

128 Véase Saleh, Felipe. "Banco Unificado de Datos: historia del fracaso de un proyecto estrella contra la delincuencia", El Mostrador, 14 de junio 2018. Disponible en:
http://www.elmostrador.cl/noticias/pais/2018/06/14/banco-unificado-de-datos-historia-del-fracaso-de-un-proyecto-estrella-contra-la-delincuencia/

129 "Transantiago: evalúan instalar cámaras de reconocimiento facial para frenar evasión". 24 de mayo del 2017.
http://www.latercera.com/noticia/transantiago-evaluan-instalar-camaras-reconocimiento-facial-frenar-evasion/

3.6.4.Colombia

En Colombia los datos biométricos se encuentran clasificados expresamente como datos sensibles por la Ley de protección de datos personales (art. 5 Ley estatutaria 1581, 2012). Como tales, tienen un tratamiento especial y se exige una autorización explícita para su tratamiento, además de la imposibilidad de transferirlos sin autorización. De la misma forma, la Superintendencia Financiera de Colombia (que actúa como autoridad de protección de datos personales) establece que no pueden llevarse a cabo decisiones automatizadas que contengan datos biométricos.[130]

Dentro de las normativas que pueden ser utilizadas para la vigilancia mediante datos biométricos, podemos encontrar que la policía puede solicitar información al Archivo Nacional de Identificación (de la Registraduría Nacional del Estado Civil), el cual contiene datos biométricos de huellas dactilares y fotografías de rostro (Decreto 019 de 2012, Ley 1753 de 2015 y Resolución 3341 de 2013).[131]

Finalmente, se ha tratado de implementar sin éxito un sistema de cámaras con reconocimiento facial para el sistema de transporte masivo en Bogotá, para asegurar la seguridad de los ciudadanos.[132] Sumado a ello se está trabajando en Colombia para instalar un sistema de vigilancia biométrica para los estadios y así "verificar los antecedentes judiciales de quienes ingresen a los partidos de fútbol".[133]

Llama la atención, a pesar de las advertencias de la Superintendencia y la Fundación Karisma, que tales programas no sean discutidos mediante proyectos legislativos, teniendo en los principios de necesidad, proporcionalidad y adecuación.[134]

3.6.5.Guatemala

En Guatemala no existe una ley de protección de datos personales, por lo que no existe un reconocimiento a los datos biométricos como datos personales sensibles. La Ley de Equipos Terminales Móviles, ya examinada, permite el registro con datos biométricos de todos aquellos compradores de SIM de celulares.[135] Sumado a ello, se ha denunciado el uso de cámaras con identificación biométrica para la individualización de asistentes a manifestaciones.[136]

---

130 Red Iberoamericana de protección de datos, "Estándares de protección de datos personales", Colombia, 2017. p. 25. Disponible en: http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estandares-Proteccion-Datos-Personales-espanol.pdf

131 Véase : https://wsr.registraduria.gov.co/-Consultas-ANI-.html .

132 Fundación Karisma. Ob. Cit. pp. 21-26

133 Ibid. p. 28

134 Fundación Karisma, Ob. cit. p. 13

135 Ávila, Renata. Ob. Cit. P. 29

136 Ibid. p. 31

3.6.6.México

El marco normativo mexicano establece estándares de protección a los datos personales. Si bien no existe una protección expresa a los datos biométricos, el INAI ha señalado que tanto la Ley federal de protección de datos personales en posesión de particulares –aplicable al sector privado y publicada el 5 de julio de 2010–, como la Ley general de protección de datos personales en posesión de sujetos obligados –aplicable al sector público y publicada el 26 de enero de 2016– tienen una protección especial, por tratarse de datos sensibles.[137]

Dentro del ordenamiento jurídico federal no podemos encontrar normativa que se refieran a la utilización de datos biométricos para la vigilancia. No obstante, a nivel estadual podemos encontrar la normativa de Jalisco que regula el "centro de monitoreo, video vigilancia, biometría y cabina".[138] En ella se establece que debe recabarse los datos dactilares y facial a todas las personas que hayan ingresado a la cárcel (art. 36, Reglamento para el centro de monitoreo, video vigilancia, biometría y cabina), la que permitirá ayudar a "autoridades competente" a detectar a todas aquellas personas que generen avisos por alguna causa penal (art. 38); del mismo modo, "cuando realicen detenciones, el Personal Operativo del Centro deberá consultar las bases de datos de información criminal incluyendo el equipo biométrico, para verificar si el detenido cuenta con antecedentes y, en su caso lo harán del conocimiento de la autoridad a la que se ponga a disposición el detenido" (art. 39).

137 INAI, "Guía para el tratamiento de datos biométricos", Ciudad de México, Marzo 2018. p. 19

138 Disponible en: http://www.sayula.gob.mx/reglamentosPDF/REGLAMENTO%20DEL%20CENTRO%20DE%20MONITOREO.pdf

4. Conclusiones

Los países estudiados tienen legislaciones que regulan de alguna forma la vigilancia, aun cuando en ninguno de ellos existe una regulación que aborde y sistematice de forma detallada el uso de tecnologías en actividades de vigilancia. Las experiencias comparadas estudiadas dan cuenta de que existen diversas leyes y regulaciones administrativas que permiten en forma concreta el desarrollo de capacidades estatales de vigilancia en relación al uso de tecnología, en esferas tales como la actividad de inteligencia, televigilancia, interceptación de comunicaciones, retención de datos y metadatos, entre otras. De este modo, la idea de un cuerpo normativo de estándares generales que sistematicen la adquisición, el uso de las tecnologías y de los métodos de vigilancia con pleno respeto de los derechos humanos, se presenta como novedosa y requiere de un esfuerzo de discusión adicional para su desarrollo.

La dispersión normativa sobre uso de tecnologías de vigilancia por parte de agentes estatales no obsta a la aplicación transversal de principios comunes. Los principios de legalidad y proporcionalidad debieran ser los parámetros inspiradores de las políticas de vigilancia, tanto para cuerpos de inteligencia como para cuerpos de policía, independientemente de las tecnologías utilizadas. No obstante, son pocas las normativas estudiadas que hacen expresa referencia a estos principios, dejando a sus ciudadanas en una situación de indefensión frente al aparataje estatal de vigilancia cuando existe exceso e ilegalidad en su aplicación.

La constante referencia a tales principios no es antojadiza. Más bien, se trata de principios rectores para los Estados en políticas de vigilancia para hacerlas consistentes con el respeto de los derechos humanos. Así ha sido repetidamente señalado en el Sistema Interamericano de Derechos Humanos. De este modo, todos los órganos estatales deberían seguirlos, incluyendo las policías y órganos de inteligencia. Los principios de legalidad y proporcionalidad permiten a los órganos de persecución penal y de inteligencia instruirlos en cómo actuar frente a posibles violaciones de derechos humanos; del mismo modo, permite a los jueces tener pautas normativas de cuándo es admisible (y cuándo no) intrusiones a los derechos humanos por agentes estatales que velan por la seguridad pública.

La revisión de las distintas legislaciones buscó verificar que existiera una regulación respetuosa con los derechos humanos de las personas, mediante la existencia de facultades legales expresas, como intervenciones judiciales previas y posteriores a la actuación de vigilancia, para los casos de actuaciones intrusivas que resulten lesivas de derechos fundamentales. Aunque tales exigencias parecen básicas, no se encontraron como una regla transversal en la región.

De esta manera, las legislaciones aparecen, en general, con reglas amplias y ambiguas respecto a las intromisiones que pueden ejecutar los agentes estatales y, a menudo, con silencio respecto de ciertas formas de vigilancia. Existe una gran divergencia entre legislaciones que consagran una regulación detallada de ciertas capacidades de vigilancia y otras que no lo consideran de manera específica, debiendo recaer en reglas y principios generales del derecho para su legalidad.

Como ha sido descrito, varios países de la región carecen de protección judicial previa frente al acceso a ciertos datos, incluidos los datos biométricos (datos personales sensibles), los datos y metadatos retenidos por ISP (entre ellos geolocalización), y la información obtenida

mediante uso de televigilancia. Del mismo modo, una revisión judicial posterior (de oficio o a instancias de la contraparte en un eventual procedimiento judicial) es poco habitual.

Lo anterior responde, en parte, a la falta de preparación de los legisladores frente a las nuevas dimensiones que ha adquirido el uso de la tecnología y su impacto en la privacidad en la era digital, como también a la voluntad de los Estados de valerse de la tecnología para adquirir mayor poder y control frente a sus ciudadanos.

Muchas de las tecnologías aquí descritas cuentan con capacidad para contribuir a enfrentar problemas de seguridad pública que conforman parte de la tarea esencial de los Estados, por lo cual muchos de ellos han iniciado una espiral de implementación masiva de las mismas. En cada uno de esos casos, los Estados carecen de una evaluación del impacto que pueden tener en el ejercicio de otros derechos humanos como la privacidad, la libertad de expresión, el derecho a reunión y el derecho a no ser discriminado. A pesar del potencial para afectar esos derechos, no se verificaron reglas especiales para la adquisición de estas tecnologías.

Cualquier beneficio que el uso de tecnologías de vigilancia para fines de seguridad pública debe considerar en el diseño e implementación de programas que las incorporan, mecanismos de balance y proporcionalidad de afectación de tales derechos, y contemplar mecanismos de transparencia y control efectivo que permitan a la ciudadanía ejercer sus derechos frente a los abusos que se cometan. Ello hace necesario revisar las normas que aplican a su adquisición, implementación, uso y control.


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina