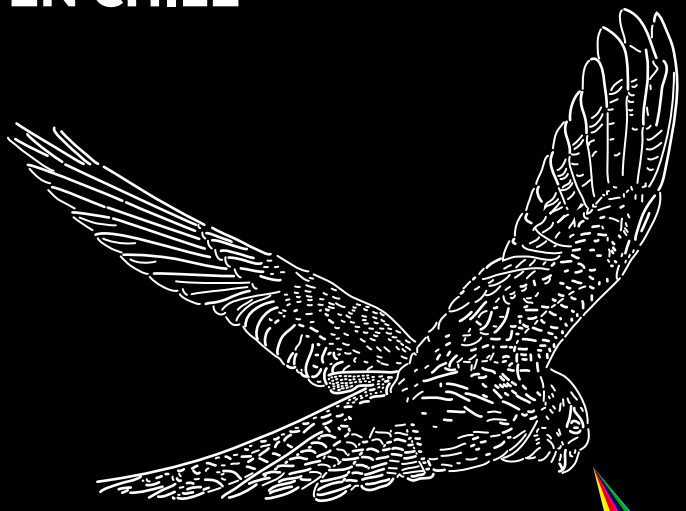
PROPUESTA DE ESTÁNDARES LEGALES PARA LA VIGILANCIA EN CHILE

DERECHOS DIGITALES
América Latina



MARÍA PAZ CANALES
JUAN CARLOS LARA

LA CONSTRUCCIÓN DE ESTÁNDARES LEGALES PARA LA VIGILANCIA EN AMÉRICA LATINA

PARTE III: PROPUESTA DE ESTÁNDARES LEGALES PARA LA VIGILANCIA EN CHILE

MARÍA PAZ CANALES
JUAN CARLOS LARA

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

Esta publicación fue posible gracias al apoyo de Privacy International

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.

Contenido

I. Introducción

La regulación de la vigilancia estatal constituye uno de los desafíos más significativos planteados por la irrupción de las tecnologías de comunicación: aunque esperamos que el aparato estatal mantenga la seguridad, su capacidad de buscar esos fines infringiendo la privacidad crece sin una respuesta normativa.

A pesar de que organizaciones de la sociedad civil a nivel global y órganos especializados a nivel internacional han realizado denodados esfuerzos por fijar principios y estándares para un ejercicio de la vigilancia respetuoso de los derechos humanos, ese desarrollo no ha permeado a la legislación a nivel local en Chile y en América Latina. Es más, escándalos recientes, como el caso en torno a la Operación Huracán y una serie de reportes periodísticos sobre escuchas telefónicas ilegales por parte de funcionarios policiales, reflejan la limitada comprensión de las capacidades de la tecnología por parte de algunos órganos, que da como resultado la extensión del uso de la tecnología de vigilancia sin transparencia y sin rendición de cuentas, afectando intensamente los derechos fundamentales de un gran número de personas.

El presente texto, el tercero en una breve serie que Derechos Digitales ha dedicado al delicado tema de la regulación de la vigilancia estatal, recoge esas preocupaciones con el fin de convertirlas en puntos de acción concretos. Los mecanismos discutidos implican actualizar la normativa vigente, establecer y actualizar los protocolos existentes o sugerir aquellos que debieran dictarse, y mejorar los comportamientos de múltiples partes involucradas en la actividad estatal de vigilancia y recolección de información.

Estas recomendaciones pretenden guiar la acción estatal en un conjunto de puntos críticos, donde el sistema normativo todavía no cumple con los estándares provenientes de principios fundamentales de democracia, dignidad y libertad, y del desarrollo del derecho internacional de los derechos humanos. Para llegar a estas recomendaciones, Derechos Digitales ha conducido una investigación amplia y profunda, haciendo una extensa revisión de bibliografía, revisando legislación comparada, consultando con especialistas, y construyendo en la medida de lo posible instancias de diálogo entre conocedores y operadores del sistema. Hemos abierto la conversación y unido puntos comunes de aprehensión, para formular nuestras propuestas de los cambios que el ordenamiento jurídico chileno necesita para salir del rezago en el resguardo de los derechos fundamentales frente a la creciente capacidad de intrusión del Estado.

II. Marco de derechos humanos y obligaciones internacionales para la construcción de estándares legales en materia de vigilancia

1. Normas internacionales que obligan a Chile en materia de vigilancia

Las prácticas de vigilancia, por su propia naturaleza, son ordinariamente capaces de vulnerar derechos humanos como la protección de la intimidad, el debido proceso o la libertad ambulatoria. Por lo mismo, acciones del propio Estado pueden directa o indirectamente afectar no solamente intereses individuales o colectivos, sino también infringir obligaciones propias del derecho internacional de los derechos humanos, contenidas en los tratados internacionales suscritos y ratificados por Chile.

Chile es signatario y está obligado por los siguientes tratados internacionales:

- El **Pacto Internacional de Deberes Civiles y Políticos** (PIDCP), vigente en Chile desde el 29 de abril de 1989. Contempla derechos potencialmente afectados por la vigilancia estatal en las obligaciones de respeto a los derechos a la libertad y seguridad de la persona (artículo 9), debido proceso (art. 14), privacidad (art. 17), libertad de pensamiento, conciencia y religión (art. 18), libertad de expresión (art. 19), libertad de reunión pacífica (art. 21) y libertad de asociación (art. 22); también en general, el derecho a igual protección de los derechos reconocidos y el derecho al recurso judicial (art. 2).
- La **Convención Americana sobre Derechos Humanos** (CADH), vigente en Chile desde el 5 de enero de 1991, firmada en el seno de la Organización de Estados Americanos (OEA). Reconoce los derechos a la libertad y seguridad personal (art. 7), debido proceso (art. 8), privacidad (art. 11), libertad de conciencia y religión (art. 12), libertad de pensamiento y de expresión (art. 13), derecho de reunión (art. 15) y libertad de asociación (art. 16); también, el derecho al recurso judicial (art. 25). Son órganos encargados la Comisión Interamericana de Derechos Humanos y la Corte Interamericana de Derechos Humanos.
- La **Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial**, vigente en Chile desde el 12 de noviembre de 1971. Dispone en general obligaciones contra un tratamiento desigual basado en razones de raza, color u origen nacional o étnico, y obliga a prevenir y combatir prácticas discriminatorias por parte del Estado que resulten en un desigual ejercicio de derechos fundamentales.
- La **Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer**, vigente en Chile desde el 9 de diciembre de 1989. Busca la prevención y el combate a toda distinción o discriminación hecha con fundamento en el género y que tenga el propósito o el efecto de producir una afectación negativa en el ejercicio de derechos por las mujeres, en cualquier ámbito, no restringido a la actividad estatal. Se suma a esos esfuerzos lo comprometido en términos afines en la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia

Contra la Mujer, también denominada **Convención de Belém do Pará**, vigente en Chile desde noviembre de 1998, y firmada en el seno de la OEA.

- La **Convención sobre los Derechos del Niño**, vigente en Chile desde el 27 de septiembre de 1990. Busca el resguardo de los derechos e intereses de todas las personas menores de 18 años, en condiciones de no discriminación y de protección de su desarrollo integral. Reconoce de manera especial los derechos a la no discriminación (art. 2), libertad de expresión (art. 13), libertad de conciencia y religión (art. 14), libertad de asociación (art. 15) y privacidad (art. 16).
- La **Constitución y el Convenio de la Unión Internacional de las Comunicaciones** (UIT), que Chile suscribió en 1982. La Constitución de la UIT reconoce el derecho del público a utilizar el servicio internacional de telecomunicaciones (art. 33), así como también el deber de los Estados parte de resguardar el secreto de las telecomunicaciones, con la posible excepción de su comunicación en cumplimiento de la ley (art. 37). Aunque el lenguaje utilizado por los textos acordados es propio de su origen como acuerdo de comunicaciones telegráficas en el siglo XIX, sus reglas se extienden en general a las comunicaciones a distancia.

Además, Chile es signatario de otros acuerdos, quedando obligado a su cumplimiento y, en su caso, a implementar sus normas en legislación interna. Ellos incluyen:

- La **Convención Interamericana sobre Asistencia Mutua en Materia Penal** (CIAAMP), vigente en Chile desde julio de 2004. Constituye el marco jurídico por el cual los Estados parte comprometen prestarse asistencia mutua en investigaciones, juicios y actuaciones en materia penal, referente a delitos cuyo conocimiento sea de competencia del Estado requirente al momento de solicitarse la asistencia, incluyendo la asistencia en la realización de peritajes y entrega de información solicitada por el Estado requirente (art. 7). Solamente los Estados (no así los intervinientes en juicio) pueden invocar sus normas. Requiere cierta gravedad de los delitos (art. 6), exigiendo penalidad de un año para que proceda la asistencia mutua. No exige la doble incriminación (esto es, que el delito sea igualmente punible para la ley del Estado requerido), pero en caso de no haberla, permite no brindar asistencia si la solicitud se refiere a las medidas de embargo y secuestro de bienes e inspecciones y allanamientos (art. 5).
- Además de la CIAMMP, Chile ha firmado varios otros acuerdos de asistencia legal mutua (o "MLATs", por la sigla en inglés de *mutual legal assistance treaty*). Ellos incluyen una serie de acuerdos bilaterales con buena parte de los países de las Américas y el Caribe, centrados principalmente en el intercambio de información con fines de combate al narcotráfico.[1] Destaca también la firma por Chile de la Convención Europea de Asistencia Mutua en Materia Penal, vigente desde 2012, que permite el intercambio de información y otras diligencias de investigación con países que son parte del Consejo de Europa. También el Acuerdo en Materia de Incremento de

1 Red Hemisférica de Cooperación Jurídica en Materia Penal. Disponible en: http://web.oas.org/mla/es/paginas/countries_bilateral.aspx?ISO=CHL

la Cooperación en la Prevención y Combate del Delito Grave, suscrito entre Chile y Estados Unidos, vigente desde 2014, que autoriza el intercambio de información en la investigación de "delitos graves", sin necesidad de autorización judicial.

- El Convenio sobre la Ciberdelincuencia de 2001, o **Convenio de Budapest**, vigente desde agosto de 2017, y pendiente de implementación por ley. Busca armonizar las reglas de sanción y persecución de ciberdelitos, consagrando nuevos tipos penales y reglas de cooperación internacional. Entre otros delitos, sanciona el acceso ilícito a sistemas informáticos (art. 2), la interceptación ilícita de comunicaciones informáticas privadas (art. 3), y los ataques a la integridad de los datos (art. 4). Además, autoriza a los Estados parte a regular la interceptación de comunicaciones como parte de la investigación (art. 21), y dedica su Capítulo III a las reglas de asistencia mutua entre Estados parte para la persecución de ciberdelitos.
- El **Acuerdo de Asociación entre la República de Chile, por una parte, y la Comunidad Europea y sus Estados Miembros, por otra,** vigente desde 2003. En el Acuerdo, Chile y la Unión Europea acuerdan cooperar para mejorar los niveles de protección de datos personales y evitar barreras al comercio para su intercambio (art. 30).

Finalmente, merecen mención los compromisos que guían al Estado de Chile ante la comunidad internacional, fuera del derecho de los tratados; no con carácter vinculante que pueda ser oponible frente a los demás Estados, sino como muestra del compromiso que es exigible por parte de sus propias ciudadanas, o como recomendaciones expertas de los órganos de protección de derechos humanos. Se encuentran entre ellos:

- La **Declaración Universal de los Derechos Humanos**, de 1948, que incluye reconocimiento fundacional de los derechos a la libertad y seguridad (art. 3), a la igual protección de la ley (art. 7), al recurso judicial (art. 8), al debido proceso (art. 10 y 11), a la privacidad (art. 12), a la libertad ambulatoria (art. 13), a la libertad de expresión (art. 19), a las libertades de reunión y asociación (art. 20). Es reconocido continuamente por el Estado chileno en la suscripción de otros acuerdos de distinta naturaleza.
- La **Declaración Americana de los Derechos y Deberes del Hombre**, también de 1948, aprobada por la Novena Conferencia Internacional Americana en Bogotá. Reconoce los derechos a la libertad y seguridad de la persona (art. I), a la igualdad (art. II), a la libertad de expresión (art. IV), a la protección de la vida privada (art. V), y a la inviolabilidad del domicilio y la correspondencia (arts. IX y X).
- La **Resolución Nº 68/167 sobre el Derecho a la Privacidad en la Era Digital**, adoptada por la Asamblea General de las Naciones Unidas el 18 de diciembre de 2013, y firmada también por Chile.[2] Mediante la resolución, la Asamblea General exhorta a los Estados a examinar y revisar sus prácticas y reglas de vigilancia e interceptación de comunicaciones, velando por dar pleno cumplimiento a las obligaciones nacidas del derecho internacional de los derechos humanos. También, a establecer meca-

2 Asamblea General de las Naciones Unidas, Resolución 68/167, El derecho a la privacidad en la era digital, A /C.3/71/L.39. Disponible en: https://undocs.org/es/A/RES/68/167.

nismos de transparencia y rendición de cuentas para las actividades de vigilancia y recolección de datos.

- La **Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión**, de 21 de junio de 2013, pronunciada por el Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA. Mediante la declaración, los relatores manifiestan como programas secretos de vigilancia destinados a la lucha contra el terrorismo y a la defensa de la seguridad nacional podrían afectar de manera severa el derecho a la libertad de pensamiento y expresión, y el derecho a la intimidad de las personas.

Recomiendan garantizar la seguridad nacional con arreglo a estándares internacionales en materia de derechos humanos; y señalan que "los Estados deben garantizar que la intervención, recolección y uso de información personal, incluidas todas las limitaciones al derecho de la persona afectada a acceder a información sobre las mismas, estén claramente autorizadas por la ley a fin de proteger a la persona contra interferencias arbitrarias o abusivas en sus intereses privados.
La ley deberá establecer límites respecto a la naturaleza, alcance y duración de este tipo de medidas, las razones para ordenarlas, las autoridades competentes para autorizar, ejecutar y supervisarlas y los mecanismos legales para su impugnación".[3]

Además "[l]as leyes deben asegurar que el público pueda acceder a información sobre los programas de vigilancia de comunicaciones privadas, su alcance y los controles existentes para garantizar que no puedan ser usados de manera arbitraria. En consecuencia, los Estados deben difundir, por lo menos, información relativa al marco regulatorio de los programas de vigilancia; los órganos encargados para implementar y supervisar dichos programas; los procedimientos de autorización, de selección de objetivos y de manejo de datos, así como información sobre el uso de estas técnicas, incluidos datos agregados sobre su alcance. En todo caso, los Estados deben establecer mecanismos de control independientes capaces de asegurar transparencia y rendición de cuentas sobre estos programas".[4]

2. Normas constitucionales relevantes

La Constitución Política de la República de Chile, vigente desde 1980 y reformada en múltiples ocasiones, contempla, en términos relevantes para la regulación y despliegue de actividades de vigilancia, lo siguiente:

- La declaración inicial de consagración de las condiciones de libertad, igualdad

---

3 Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión Disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2, párrafo 8.

4 Ibid, párrafo 12.

y dignidad, junto al deber del Estado de resguardar la seguridad nacional, en el artículo 1º.

- La limitación del ejercicio de la soberanía por la prevalencia de los "derechos esenciales", incluyendo el deber del Estado de respetar y promover los derechos garantizados por la Constitución y por los tratados internacionales ratificados por Chile (art. 5º). Con esto, todo el rango de derechos fundamentales presentes en tratados internacionales, aun si no son parte del texto explícito de la Constitución, pasan a ser parte del ordenamiento jurídico.
- El derecho a la libertad individual y la seguridad personal, en el artículo 19, Nº 7.
- El derecho al respeto y la protección de la vida privada, y de los datos personales, en el artículo 19, Nº 4.
- La inviolabilidad de las comunicaciones privadas, en el artículo 19, Nº 5, autorizando restricciones reguladas por ley.
- La protección de los datos personales, en el artículo 19, Nº 4.
- El derecho a la libertad de emitir opinión e información, sin censura previa, en el artículo 19, Nº 12, autorizando restricciones reguladas por ley.
- El derecho de reunión pacífica sin permiso previo, en el artículo 19, Nº 13.
- El derecho de asociación sin permiso previo, en el artículo 19, Nº 15.
- El derecho al debido proceso, en el artículo 19, Nº 7, con directas remisiones al principio de legalidad.
- El derecho de acceso a la jurisdicción para la presentación de recursos, en el artículo 19, Nº 3.
- La protección de la esencia de las garantías, en el artículo 19, Nº 26, que establece que los derechos garantizados por la Constitución no pueden ser afectados en su contenido esencial al regularse por ley, resguardando así contra restricciones desproporcionadas establecidas legalmente.

III. Principios a ser recogidos transversalmente en materia de vigilancia

Una formulación de estándares normativos para la vigilancia debe considerar principios y normas de derecho internacional en materia de derechos humanos y la experiencia desarrollada por la jurisprudencia comparada en la aplicación de los mismos, como también el desarrollo de principios formulados desde los múltiples interesados, incluida la sociedad civil organizada a nivel global.[5] Todo lo anterior, que puede ser encontrado en las Partes I y II de la investigación que hemos denominado "La construcción de estándares legales para la vigilancia en América Latina", se plasma a continuación en la forma de principios que emanan como relevantes y transversales para la regulación de tecnologías de vigilancia que han sido objeto de estudio en el campo de: actividades de inteligencia, interceptación de comunicaciones (con fines de inteligencia o persecusión penal), retención de data y metadata por proveedores de servicios de comunicaciones, uso de sistemas de televigilancia e implementación de tecnologías biométricas.

1. Legalidad

El principio de legalidad debe inspirar las actuaciones estatales que implican el uso de tecnologías de vigilancia que sean intrusivas y lesivas de otros derechos humanos, tales como la privacidad, la libertad de expresión, el derecho a reunión y el derecho a no ser discriminado. El principio de legalidad exige que las causales de justificación de medidas intrusivas a través del uso de tecnologías de vigilancia sean taxativas y claramente señaladas en la ley. Conforme a nuestra Constitución Política, cualquier limitación a los derechos humanos debe ser prescrita por ley.

La ley debe cumplir además con un estándar de claridad y precisión suficientes para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación. Es esencial contar con reglas claras y detalladas sobre medidas de vigilancia, especialmente dado que la tecnología disponible para su uso se está volviendo cada vez más sofisticada. La legislación nacional debe ser suficientemente clara para proporcionar a los ciudadanos una indicación adecuada de las circunstancias y las condiciones en que las autoridades públicas están facultadas para recurrir a tales medidas.

Para determinar la procedencia de una medida de vigilancia debe atenderse a la naturaleza de los delitos concernidos; contemplar una definición clara de las categorías de personas que pueden ser objeto de la medida; consagrar un límite en la duración de la vigilancia; el procedimiento a seguir para examinar, usar y almacenar los datos obtenidos; las precauciones que deben tomarse al comunicar los datos a otras partes; y, las circunstancias en las cuales los datos obtenidos pueden o deben ser borrados o destruidos.

---

5 Varios de los principios que a continuación se presentan, toman, adaptan y complementan el contenido de Necesarios & Proporcionados: Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Disponibles en: https://necessaryandproportionate.org/es/necesarios-proporcionados

La ley debe indicar el alcance de cualquier facultad discrecional conferida a las autoridades competentes y la forma de su ejercicio con suficiente claridad para brindar al individuo una protección adecuada contra la interferencia arbitraria.

El uso de tecnologías de vigilancia solo puede resultar procedente para perseguir fines legítimos del Estado y que sean necesarios en una sociedad democrática. En cualquier caso, debe ceñirse siempre a los principios de necesidad, idoneidad y proporcional en sentido estricto, teniendo en consideración la afectación de derechos fundamentales y evitando cualquier forma de discriminación arbitraria en su aplicación. Lo anterior debe resultar vinculante, tanto para los organismos que solicitan medidas intrusivas como para los órganos judiciales que las otorgan.

2. Necesidad

La vigilancia debe limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo. La vigilancia solo debe ser autorizada cuando es el único medio para alcanzar el objetivo legítimo, o el menos propenso a vulnerar los derechos humanos de los que estén disponibles. La carga de establecer esta justificación, tanto en los procesos judiciales como en los legislativos, recae en el Estado.

La disponibilidad a un costo relativamente bajo no es suficiente para justificar el uso de la tecnología de vigilancia. Los órganos públicos deben abstenerse simplemente de tomar la decisión que parece ser la menos costosa, la más fácil y la más rápida, pero que no tiene en cuenta el impacto en los intereses legítimos de los ciudadanos y el efecto sobre sus derechos fundamentales.

3. Idoneidad

Los casos de vigilancia autorizados por ley deben ser apropiados para cumplir el objetivo legítimo específico identificado.

Los sistemas de vigilancia no deben usarse si hay alternativas adecuadas disponibles. Una alternativa debiera considerarse como adecuada cuando no resulte significativamente menos efectiva que el sistema de vigilancia o implique costos comparativamente desproporcionados.

4. Proporcionalidad

Dado que la vigilancia es un acto altamente intrusivo que interfiere con los derechos humanos, lo siguiente debe ser comprobado judicialmente o durante el proceso normativo de su introducción regulatoria:

a. Existe un alto grado de probabilidad de que un delito grave o una amenaza específica para un fin legítimo ha sido o será llevado a cabo.
b. Existe un alto grado de probabilidad de que las evidencias pertinentes y materiales de un delito grave o una amenaza específica para un fin legítimo se conseguirían

mediante el acceso solicitado a la información protegida.

c. Otras técnicas de investigación que son menos invasivas ya han sido agotadas o serían inútiles, de modo que la técnica usada sería la menos invasiva en la práctica.
d. La información a la que se accederá estará limitada a lo relevante y material para el delito grave o la amenaza específica al fin legítimo alegado.
e. Cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud.
f. La información será accedida solo por la autoridad específica y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización.
g. Que los datos recogidos no se utilicen posteriormente para otros fines o sean divulgados a destinatarios no previstos que podrían utilizarlos para fines adicionales e incompatibles.
h. Que las actividades de vigilancia solicitadas y técnicas propuestas no menoscaben la esencia del derecho a la privacidad o de las libertades fundamentales.

5. Debido proceso

Los procedimientos legales de vigilancia deben estar taxativa y apropiadamente enumerados en la ley, deben ser practicados consistentemente, y las reglas de aplicación deben encontrarse disponibles para el público general.

Las decisiones relacionadas con el uso de mecanismos de vigilancia requieren de un control de la legalidad, idealmente mediante la intervención sustantiva de una autoridad judicial independiente, de forma previa al despliegue de las herramientas de vigilancia.

La interceptación de comunicaciones, el acceso a datos de comunicación y la solicitud de llaves de cifrado a la persona respecto de la cual se ha autorizado la vigilancia debe solo aceptarse mediante orden judicial previa que cumpla con estándares de necesidad, idoneidad y proporcionalidad, en relación al ejercicio del derecho de defensa y en casos taxativos establecidos por ley.

El debido proceso incluye notificación de la persona respecto de la cual se autoriza la vigilancia, salvo en las siguientes circunstancias:

a. La notificación pondría en serio peligro la finalidad para la que se autoriza la vigilancia, o existe un riesgo inminente de peligro para la vida humana.
b. La autorización para retrasar la notificación es otorgada por la autoridad judicial competente en el momento en que se concede la autorización para la vigilancia.
c. El usuario afectado se notifica tan pronto como el riesgo desaparece según lo determinado por la autoridad judicial competente.

El uso de la vigilancia encubierta es altamente intrusivo debido a su naturaleza secreta. Además, tiene poco o ningún efecto preventivo. Por lo tanto, se debe evitar su uso, a menos de que se trate de asegurar evidencia bajo estándares de autorización judicial.

6. Mecanismos de control y derecho a recurso

Deben implementarse mecanismos independientes de supervisión de los sistemas de vigilancia o facultades de vigilancia que la ley autorice.

Las autoridades encargadas del control de las medidas de vigilancia deben ser independientes de las autoridades encargadas de ejecutar la vigilancia, estar capacitadas en materia de tecnología y de protección de derechos humanos, y contar con recursos suficientes para el ejercicio de su función.

Debe haber una relación inversa entre aquellas medidas de vigilancia que requieran de secreto para su efectividad, y los mecanismos para supervisar la aplicación de las medidas de vigilancia secreta, y los mecanismos de notificación y recurso previstos por la legislación. Del mismo modo las medidas de control y remedio disponible deben ser mayores en aquellos casos en que se conceda mayor arbitrio a las autoridades para ordenar medidas de vigilancia fundadas en la seguridad nacional.

La revisión y supervisión de las medidas de vigilancia secreta deben entrar en juego en tres etapas: cuando la vigilancia se ordena por primera vez, mientras se lleva a cabo y después de que se ha terminado.

La posibilidad de requerir control o ejercer un recurso no debiera estar condicionada la notificación de la medida de vigilancia, cualquier persona que crea que ha estado sometida a vigilancia secreta debiera poder presentar una solicitud.

7. Transparencia activa

El uso de herramientas y mecanismos de vigilancia debe estar acompañado de mecanismos de transparencia activa, incluyendo datos estadísticos que den información confiable a la ciudadanía y dé potestades de control de la labor de quienes ejecutan las interceptaciones de comunicaciones o acceso a datos a través de otras tecnologías, por parte de otros órganos públicos que puedan generar contrapesos efectivos al ejercicio de tales atribuciones.

Toda adquisición, desarrollo, elaboración por terceros y mantenimiento de tecnologías de vigilancia debiera pasar por estrictos controles de transparencia y seguridad, a fin de mitigar riesgos asociados a la tecnología misma.

Los propósitos de cualquier sistema de vigilancia deben comunicarse al público de modo previo a su implementación y uso, y con más detalle, por ejemplo, a través de avisos que acompañen los sistemas y la publicación de una política de uso de tecnologías de vigilancia específicas.

8. Evaluación de impacto en el ejercicio de derechos fundamentales previo a la implementación de sistemas de vigilancia

Cualquier organismo público o privado que considere la implementación de tecnologías de vigilancia debiera encontrarse obligado a realizar en forma previa una evaluación de impacto en el ejercicio de derechos fundamentales, con la participación de especialistas en tecnología, derecho, ciencias sociales, entre otras especialidades.

El objetivo de la evaluación es determinar el impacto del sistema de vigilancia que se pretenda implementar en la privacidad de los individuos y otros derechos fundamentales, con el fin de determinar si los beneficios de dicha implementación son suficientes para justificarla y, en tal caso, identificar formas de mitigar o evitar cualquier efecto adverso para los derechos identificados.

9. Debate democrático en su adopción

La adquisición y uso de tecnologías de vigilancia debe ser sometida a un control democrático que permita la construcción de confianza de la ciudadanía con el Estado.

Dado el ritmo de los cambios tecnológicos, las leyes que limitan el derecho a la privacidad deben ser objeto de debate previo a su adopción y de revisión periódica, por medio de un proceso legislativo de carácter participativo, que asegure el cumplimiento de la ponderación de derechos prescrita por la Constitución.

También en aquellos casos en que las autoridades comunales, regionales o centrales se encuentren evaluando la posibilidad de implementar tecnologías de vigilancia en el ejercicio de sus competencias, debe hacerse un esfuerzo por insertar instancias de participación de la ciudadanía, tales como consultas públicas, foros abiertos u otras.

10. Garantías para la cooperación internacional

La transferencia transfronteriza de datos recogidos como consecuencia de la implementación de tecnologías de vigilancia con fines de persecución penal deben regirse en todos los casos por los mecanismos de cooperación internacional, entre ellos los Tratados de Asistencia Legal Mutua.

El principio de la doble incriminación debe ser aplicado en el momento en que el Estado procure asistencia para efectos de hacer cumplir su legislación interna, aun si el respectivo Tratado no lo exige explícitamente.

Los acuerdos de asistencia legal recíproca y otros acuerdos de cooperación deben estar claramente documentados, a disposición del público y sujetos a las garantías de equidad procesal.

La transferencia de información a través de cooperación con agencias de inteligencia de otros países, si se admite, debe encontrarse reglada en la ley, y encontrarse sujeta a un control sustantivo estricto, por una autoridad independiente.

IV. Recomendaciones para la incorporación de estándares legales en materia de vigilancia

1. Recomendaciones dirigidas a las funciones de investigación criminal

La actividad de investigación criminal constituye, por su naturaleza, el más preclaro ejercicio de facultades de vigilancia por parte de la autoridad, que se viste con presunción de legalidad en atención a quienes la ejercen. Pero dado el carácter extremadamente intrusivo de las medidas que se sirven de la tecnología, las normas vigentes y prácticas imperantes resultan insuficientes y requieren de reformas, en los términos que se recomiendan a continuación.

i. Reglas generales

a. Órganos

El respeto a los derechos fundamentales de todas las personas afectadas por actividades de vigilancia requiere regulación de sus procedimientos, pero de manera crucial, requiere también la regulación de los órganos participantes.

Toda forma de vigilancia estatal debe ser dirigida, ejecutada y controlada, de forma exclusiva, por instituciones de investigación o persecución legal, u otras entidades con mandato específico, determinadas por ley. Todos los organismos participantes en las distintas etapas de investigación deben ser constituidos y regulados por ley, que especifique sus propósitos, sus objetivos y sus actividades autorizadas. Debe restringirse el número de posibles intervinientes con facultades para ejecutar medidas de intrusión de manera directa, o en la operación de los sistemas de interceptación de comunicaciones, recolección de datos, o vigilancia corporal.

Las autoridades encargadas del control de las medidas de vigilancia deben ser independientes de las autoridades encargadas de ejecutar la vigilancia. Su constitución y regulación deben constar en la ley, incluyendo las reglas sobre los controles procedimentales en el contexto de la investigación penal, como también las medidas de control jerárquico del cumplimiento de las reglas de procedimiento y protocolos internos. Las autoridades judiciales encargadas del control de las medidas intrusivas de investigación deben otorgar garantías de imparcialidad, competencia e independencia; deben estar capacitadas en materia de tecnología y de protección de derechos humanos, y contar con recursos suficientes para el ejercicio de su función.

Deben separarse las facultades de los órganos que hacen uso de tecnologías de vigilancia, distinguiéndose claramente aquellas que forman parte de la investigación penal y de actividad policial de las que realizan labores dentro del sistema nacional de inteligencia. Cualquier forma de comunicación de información entre ambos sistemas debiera ser de naturaleza excepcional, y encontrarse sujeta a un control sustantivo estricto, por una autoridad judicial independiente.

Los órganos encargados de la dirección y ejecución de actividades de vigilancia deben recolectar antecedentes sobre sus actividades, para la elaboración de informes estadísticos de carácter público. En particular, tratándose de actividades de vigilancia de comunicaciones, incluyendo la interceptación de comunicaciones y solicitudes de acceso a datos de comunicación (metadatos), se deben publicar informes estadísticos de manera periódica.

Tales informes deben incluir, como mínimo, información global sobre el número de solicitudes presentadas ante tribunales, en relación con la cantidad de investigaciones en curso; el número de solicitudes aprobadas y rechazadas; un desglose de la cantidad de solicitudes en relación con los proveedores de servicios que han sido destinatarios de órdenes de cooperación para la interceptación de comunicaciones; un desglose del número de solicitudes por autoridad investigadora; un desglose del tipo de intervención referida y de su propósito; y el número específico de personas afectadas por cada una y según el tipo de investigación y sus propósitos.

b. Procedimiento

Los procedimientos legales de vigilancia deben estar taxativa y apropiadamente enumerados en la ley. Esto implica que solamente las vías de investigación que hayan sido objeto de un debate democrático, que conste de un texto autoritativo que las regule, puedan ser utilizadas por parte de agentes del Estado.

Todas las medidas legalmente reguladas deben constar en reglas claras y accesibles, sin ambigüedades que den lugar a abuso. No debe entenderse que la autorización de una especie de vigilancia autoriza el uso de un género de medidas de vigilancia, ni interpretarse que todos los mecanismos tecnológicos posibles son igualmente válidos para la ejecución de una medida de vigilancia legalmente reconocida.[6]

En caso de ser útil o conveniente una medida de vigilancia o recolección de datos no reconocida legalmente, en lugar de utilizar las reglas de las medidas existentes por analogía, el resguardo y la prevención de la vulneración de derechos fundamentales exigen no proceder con la medida, ni aun con autorización judicial. Por el contrario, la inexistencia de una medida expresamente reglada en la legislación debe permitir a los cuerpos policiales y de investigación criminal manifestar sus necesidades a los órganos detentores de la potestad legislativa, a fin de iniciar el proceso de consagración y regulación. Dicho proceso debe incluir análisis de impacto, opiniones expertas y deliberación democrática, todo en condiciones de transparencia y participación.

Si una medida de investigación aparece regulada bajo menos condiciones de resguardo de principios y derechos fundamentales que otra, no debe preferirse la aplicación del texto menos protector como vía para eludir el control sobre su procedencia.

---

6 A modo de ejemplo, la capacidad de interceptar comunicaciones no implica ni conlleva la facultad de intervenir equipos o sistemas operativos completos, ni de usar técnicas maliciosas de inoculación informática.

El respeto al principio de legalidad conlleva el cumplimiento en todas las etapas de investigación de los principios que son también parte de la legislación. No es suficiente con que una medida sea "útil" a la investigación: la Constitución y los tratados internacionales ratificados por Chile exigen igualmente el análisis de su procedencia, incluyendo el examen de su idoneidad, necesidad y proporcionalidad.

La procedencia de una medida intrusiva de recolección de información contemplada en la ley debe ser calificada en relación con la naturaleza de los delitos investigados. Asimismo, la ley debe delimitar claramente las categorías de personas que pueden ser objeto de la medida, debiendo en todo caso referirse a relaciones suficientemente cercanas entre los hechos investigados y las personas afectadas por las medidas.

La ley debe consagrar un límite máximo en la duración de la vigilancia, con la capacidad de los solicitantes de las medidas para pedir prórrogas de manera fundada. La extensión temporal de las medidas de vigilancia, de incautación de objetos, de incautación de correspondencia, y cualquiera otra que signifique la tenencia de información personal y comunicaciones privadas en poder de agentes del Estado, debe ser la mínima necesaria para los fines de la investigación.

La ley debe contemplar el procedimiento para examinar, usar y almacenar los datos obtenidos, restringiendo el acceso a los mismos y resguardando su integridad, detallando las precauciones que deben tomarse al comunicar los datos a otras partes y las circunstancias en las cuales los datos obtenidos pueden o deben ser borrados o destruidos, sin perjudicar los derechos de las partes en la investigación.

La regulación debe proveer recursos procesales a favor de todas las personas cuyos derechos pudieren haber sido vulnerados.

El respeto a la legalidad implica la previsibilidad en la ejecución de las medidas de vigilancia y la uniformidad de criterios de aplicación. Los procedimientos legales de vigilancia deben ser practicados consistentemente. En consecuencia:

- Los organismos de persecución penal, como las policías y órganos técnicos encargados de llevar adelante las medidas, deben contar con protocolos, disponibles para el público general, respecto de la forma de ejecución de actividades de vigilancia y las medidas de resguardo de intereses de las personas.
- Las empresas de comunicaciones y otras que puedan ser objeto de requerimientos de la autoridad, deben contar con protocolos, disponibles para el público general, respecto de la forma de entrega de información y de resguardo de intereses de las personas.

Toda medida de investigación que implique una intrusión en la vida privada de las personas debe ser solicitada por un órgano competente y estar autorizada por un tribunal. En consecuencia, se recomienda para los órganos solicitantes de medidas de vigilancia:

- Realizar un análisis acabado de la necesidad de la ejecución de medidas de vigilancia. Las solicitudes deben estar precedidas de un examen de la pertinencia de una medida intrusiva en relación con la gravedad del hecho delictivo, de la necesidad de la medida para obtener la información necesaria, de su idoneidad para cumplir con ese fin y de la existencia de alternativas menos lesivas para los derechos de las personas involucradas.
- Solicitar por escrito la autorización a la autoridad judicial competente, resguardando que la solicitud cumpla con:
    - Especificar el delito o crimen a que se refieren, y fundamentar la procedencia de la medida haciendo referencia expresa los antecedentes que dan cuenta de su gravedad.
    - Especificar las personas a quienes se refiere, que estén estrechamente vinculadas con el delito o crimen que se está investigando, y explicando con detalle ese vínculo, haciendo referencia expresa a los antecedentes de los que se derivan las sospechas o evidencias de ese vínculo.
    - Identificar la información requerida que se busca obtener mediante la medida de vigilancia, de manera específica y con expresión de su relación con los hechos investigados. Especificar el alcance de las tecnologías dirigidas: identificar las cuentas o números de identificación de comunicaciones, las bases de datos, los dispositivos sobre los cuales se llevará adelante la información y su relación (con antecedentes fundados) con las personas respecto de quienes se investiga. Junto a ello, especificar el vínculo entre la tecnología a la que se dirige la vigilancia y la información requerida, haciendo referencia expresa a los antecedentes de los que se deriva la sospecha o evidencia de ese vínculo o la existencia de la información requerida en el dispositivo o base de datos.
    - Identificar el procedimiento de interceptación o recolección de información, explicando la metodología de vigilancia o recolección de información, el formato de almacenamiento en que será compartida a la defensa durante el proceso, el tiempo requerido para la interceptación y su justificación, y otra información que incidentalmente pudiere recibirse. Identificar los protocolos de custodia, acceso, resguardo, respaldo y eventual eliminación de la información recolectada y sus respaldos, incluyendo a las personas o instituciones involucradas en la ejecución de la medida.
    - Explicar por qué es necesaria la medida de investigación: por qué se necesita esa medida en lugar de otras, y por qué otras medidas resultarían inviables o inútiles para obtener la información requerida.
- Ser firmada por el solicitante y contener su información de contacto.
- Documentar el análisis de la pertinencia de las medidas intrusivas dentro del historial del proceso investigativo, para permitir el acceso por parte de personas afectadas y su eventual uso de recursos para remediar vulneraciones de derechos fundamentales.
- Una vez autorizada la medida, verificar que su ejecución por parte de agentes policiales se ajuste a derecho y a la autorización entregada. Verificar el respeto de las limitaciones de acceso y el cumplimiento de los protocolos de almacenamiento, uso,

respaldo y examen de la información recolectada.

- Informar a la autoridad judicial que autorizó la medida sobre toda la información adquirida durante las actividades de vigilancia y recolección de información, incluyendo su relevancia y pertinencia dentro del proceso investigativo, y sus condiciones de conservación. Informar también de posibles vulneraciones de derechos en la ejecución.
- Recolectar antecedentes para la elaboración de informes estadísticos sobre actividades de vigilancia de comunicaciones, incluyendo la interceptación de comunicaciones y la solicitud de acceso a datos de comunicación (metadatos).

En cuanto a la intervención de control por autoridad judicial, para que sea efectivo el resguardo de los derechos de los intervinientes, recomendamos:

- De forma previa al otorgamiento de la autorización:
  - Verificar la procedencia y el mérito de la solicitud en atención a todos los antecedentes presentados en la solicitud de autorización de medidas intrusivas, incluyendo el análisis del ajuste de la medida a los principios de legalidad, proporcionalidad y necesidad, las posibles alternativas para la obtención de información, y los posibles efectos de las medidas solicitadas en el ejercicio de derechos fundamentales.
  - Verificar la procedencia de la solicitud en razón de su territorio jurisdiccional. Debe prevenirse que ciertos tribunales o jueces sean preferidos por los solicitantes en razón de la deferencia que se les otorga en la solicitud de autorizaciones de intrusión. El rol de los mecanismos de transparencia activa en cuanto a solicitudes resulta esencial para sacar a la luz este tipo de situaciones.
  - Examinar la viabilidad tecnológica de las medidas especificadas. Si la solicitud no es específica respecto de los mecanismos y la metodología a través de las cuales se obtendrá la información, deberá ordenarse al solicitante que complemente o aclare su solicitud, o la solicitud deberá rechazarse.
  - Examinar si las personas sobre quienes se ejercería vigilancia se encuentran en situación de vulnerabilidad o discriminación sistemática, o si se trata de menores de edad.
- Emitir la resolución sobre autorización por escrito, asegurando que la resolución cumpla con:
  - Referir expresamente a los antecedentes presentados en la solicitud de autorización, incluyendo los hechos que se investigan y las normas legales presuntamente infringidas, para facilitar su control de legalidad.
  - Referir expresamente al análisis de los antecedentes presentados en la solicitud de autorización. En particular, si los antecedentes constituyen información fidedigna, obtenida de forma lícita, atingente a la investigación en curso.
  - Fundamentar la decisión sobre el otorgamiento de la autorización, en función del análisis de los antecedentes presentados en la solicitud de autorización y en razón de la legalidad, necesidad, idoneidad y proporcionalidad de la medida solicitada en relación con los hechos investigados.

- En caso de autorizar la medida, especificar el alcance de la misma, identificando los nombres o números de cuentas de servicios de comunicación o de almacenamiento de datos, o los dispositivos o sistemas informáticos a que se refiere; el método particular de vigilancia o recolección de información autorizado, y el período de tiempo a que se extiende la medida. En lo sustantivo, la autoridad judicial debe limitar el alcance en la ejecución de la medida a la información no pertinente a la que se acceda de manera incidental. Debe además ordenar un período limitado de mantención de la información recolectada, que no supere los fines del procedimiento.
- En caso de autorizar la medida, ordenar la finalización anticipada de la misma una vez obtenida la información requerida por el solicitante.
- En caso de autorizar la medida, ordenar al solicitante informar, de manera completa y fidedigna, sobre toda la información recibida durante el proceso de vigilancia o recolección de información, incluyendo el cumplimiento de los protocolos de acceso, custodia y eliminación. Además, ordenar al solicitante informar de manera fundada sobre la necesidad de conservación del secreto de las actuaciones de investigación.

- Una vez otorgada la medida, solicitar información continua de parte del solicitante sobre las condiciones de ejecución de las medidas intrusivas. Verificar el ajuste a derecho de las actividades de vigilancia y recolección de información que lleguen a su conocimiento en tanto tribunal competente para conocer de los hechos investigados.
- Una vez finalizado el plazo de ejecución de la medida, disponer el fin del secreto de la misma, si procediere y no afectare a los fines de la investigación. Del mismo modo, ordenar la notificación de las personas afectadas por las actividades de vigilancia.

Toda persona que ha sido objeto de actividades de vigilancia, ya sea sobre sus comunicaciones, sus objetos o su información contenida en sistemas propios o ajenos, tiene derecho a ser comunicada de haber sido objeto de vigilancia. En consecuencia, se recomienda:

- Reconocer el derecho de la persona afectada por vigilancia de recibir una notificación, por escrito, por parte de la autoridad a cargo de las medidas intrusivas, de la resolución que autoriza actividades de vigilancia que le afectan, a la brevedad posible. Tal notificación debe incluir:
  - Información sobre los hechos que se investigan y las sospechas sobre la vinculación de los mismos con la persona afectada, y sus comunicaciones o sus efectos personales afectados, en lenguaje claro y comprensible.
  - Información sobre el método tecnológico utilizado y los bienes y comunicaciones afectados; sobre los protocolos seguidos para el manejo de información, y sobre las personas responsables de la ejecución de las medidas.
  - Información sobre el período temporal de ejecución de la medida.
  - Información sobre la base normativa para el ejercicio de estas actividades de vigilancia, consistentes con lo autorizado por la autoridad judicial.
  - Información sobre las acciones legales y administrativas procedentes para la

rectificación o eliminación de información o de registros de comunicaciones, para la restitución de datos o de bienes incautados, y para la obtención de indemnización en caso de ser procedente.

- Reconocer como únicas posibles razones para retrasar la notificación de las personas afectadas:
    - Que la notificación pondría en serio peligro la finalidad para la que se autoriza la vigilancia, o que existe un riesgo inminente de peligro para la vida humana; por ejemplo en el caso en que sea estrictamente necesario para la investigación que la persona afectada esté temporalmente en desconocimiento de la medida intrusiva.
    - Que la autorización para retrasar la notificación es otorgada por la autoridad judicial competente en el momento en que se concede la autorización para la vigilancia.

En tales casos, la persona afectada deberá ser notificada tan pronto como el riesgo de pérdida de información o de perjuicio serio a la investigación desaparezcan, según lo determinado por la autoridad judicial competente.

- Reconocer que la posibilidad de requerir control o ejercer un recurso no debiera estar condicionada a la notificación de la medida de vigilancia. En tal sentido, cualquier persona que crea que ha estado sometida a vigilancia secreta debiera poder presentar una solicitud ante tribunales, y recibir información completa y fidedigna sobre la conducción de medidas intrusivas que le afecten.

ii. Reglas específicas

a. Interceptación de comunicaciones

La interceptación de las comunicaciones que sostiene una persona es una de las formas más intensas de afectación de la intimidad y la autonomía. Es intrínsecamente lesiva de derechos fundamentales, por lo que su procedencia debe estar sujeta a las reglas más estrictas de control. En la opinión de algunos de los actores del sistema consultados por Derechos Digitales, dentro de la investigación de campo que deriva en el presente documento, el sistema de interceptación de comunicaciones, y en particular el uso de escuchas telefónicas, carece de suficientes condiciones de uniformidad en su aplicación y de condiciones de control frente a la posibilidad de abuso.

Por lo que adicionalmente a lo indicado en la sección de reglas generales anterior, se recomienda incorporar normas legales que obliguen a los órganos de persecución penal autorizados para solicitar la interceptación telefónica a que cumplan con lo siguiente:

- Al solicitar interceptaciones de comunicaciones privadas:
    - Verificar la existencia de vías menos lesivas de recolección de antecedentes probatorios.
    - Identificar de manera precisa a las personas que serán objeto de intercepta-

ción, fundamentando la participación de cada una de ellas en los hechos que se investigan.
    - Identificar de manera específica las cuentas de servicios informáticos o números telefónicos respecto de los que se pide interceptación. Aportar antecedentes claros y fidedignos sobre la pertenencia o relación de esas cuentas con las personas a las que se refiere.
    - Identificar de manera específica los organismos encargados de la ejecución de la interceptación, y la metodología de interceptación y almacenamiento. Debiera prohibirse expresamente la utilización desoftware malicioso que aproveche vulnerabilidades técnicas de los dispositivos receptores de las comunicaciones intervenidas.
    - Aportar antecedentes precisos de hecho que justifiquen la procedencia de la medida de interceptación de comunicación, atendida la gravedad del presunto delito, o la procedencia en la persecución de los delitos señalados en otras leyes según lo dispuesto en el art. 226 bis del Código Procesal Penal.
- Al ejecutarse las interceptaciones:
    - Fiscalizar el respeto efectivo de las limitaciones de acceso, verificando que las personas con acceso a las interceptaciones sean solamente aquellas autorizadas.
    - Verificar el cumplimiento de los protocolos de almacenamiento, uso, respaldo y examen de la información recolectada. Verificar que todos los registros contengan información completa sobre las comunicaciones a que se refieren, con sus fechas y horas.
- Finalizado el período de interceptación:
    - Informar a la autoridad judicial que autorizó la medida sobre toda la información adquirida durante las actividades de vigilancia y recolección de información. Informar también de posibles vulneraciones de derechos en la ejecución.
    - Al incorporar registros de interceptación a la investigación, identificar los registros utilizados, incluyendo la mención a su relevancia y pertinencia dentro del proceso investigativo.
    - Desde el momento de la formalización de la investigación, poner a disposición todos los registros no acompañados en la investigación para su uso por las personas investigadas y su defensa, utilizar formatos que permitan un conocimiento rápido de los contenidos de los registros, identificando de manera precisa y completa cada una de las comunicaciones aportadas.

Los tribunales deben también cumplir con su función de control de las actividades de investigación y de resguardo de los derechos fundamentales de todos los intervinientes en el proceso penal. Esto obliga a revisar cada solicitud en detalle, en lugar de entregar autorizaciones de lesión de derechos fundamentales basadas solamente en los relatos de los solicitantes de las medidas. En consecuencia, adicionalmente a lo indicado en la sección de reglas generales anterior, se recomienda la introducción de directrices en el sentido siguiente:

- Ante una solicitud de autorización de interceptación de comunicaciones:
    - Ponderar cuidadosamente los antecedentes presentados por el solicitante y el mérito de la solicitud. En particular, realizar un análisis preliminar sobre el carácter de los hechos alegados como constitutivos de delitos que permitan una medida intrusiva; revisar con cuidado si los antecedentes aportados permiten sostener una sospecha fundada.
    - Analizar con cuidado la forma de interceptación y la metodología descrita por el solicitante. Verificar que la forma técnica de interceptación se ajuste a derecho y no comprometa la seguridad o la integridad de los equipos ni de los sistemas de comunicación. Asegurarse de que existe una explicación cabal de la misma, y de que la misma sea comprensible para terceras personas, incluidas las personas investigadas y sus defensas, con miras a su eventual notificación. Asegurarse de comprender el funcionamiento de la metodología descrita, su viabilidad y los riesgos asociados, consultando con especialistas si fuere necesario.
    - Requerir información adicional por parte del solicitante, si fuere necesario, sobre los antecedentes fundantes de la solicitud o sobre la forma y metodología de interceptación.
- Al emitir la resolución que autoriza la interceptación:
    - Fundamentar la decisión de autorización, explicando la ponderación de derechos y las circunstancias que hacen necesaria e idónea la medida de interceptación de comunicaciones.
    - Ordenar la entrega de informes al tribunal sobre: todos los registros que se realicen, debidamente identificados; y el cumplimiento de todos los protocolos y medidas técnicas y organizativas para la limitación en el acceso a las comunicaciones interceptadas y sus respaldos, y para la prevención de acceso por personas no autorizadas.
- Finalizado el plazo de interceptación de comunicaciones:
    - Ordenar al solicitante que informe sobre la totalidad de los registros autorizados, con desglose de las cuentas y números intervenidos, y las personas identificadas en las comunicaciones.
    - En caso de existir interceptaciones no autorizadas, ordenar su exclusión como medio probatorio y ordenar la destrucción de los registros existentes, dejando constancia por escrito a fin de permitir el inicio de acciones legales por parte de las personas afectadas.

b. Solicitudes de acceso a correos y mensajes almacenados

La práctica en la investigación criminal en Chile, según lo recopilado en la investigación de campo por parte de Derechos Digitales, muestra un uso extendido de la medida investigativa de incautación de correo, contenida y regulada en el artículo 218 del Código Procesal Penal, como base investigativa para la incautación de copias digitales de correos electrónicos. No obstante, dicha disposición mantiene requisitos de procedencia bajos: se permite la adopción

de la medida previa autorización judicial, a solicitud fundada del fiscal, cuando por motivos fundados fuere previsible la utilidad de la correspondencia para la investigación.

La disparidad con los requisitos para la interceptación de comunicaciones privadas es dramática. No se requieren fundadas sospechas, basadas en hechos determinados; no se exige que la investigación se refiera a hechos con el carácter de crimen o delito grave; no se requiere que la incautación de correos sea imprescindible para la investigación, sino que se prevea su mera utilidad. Esa disparidad es a su vez incongruente con normas supralegales: la correspondencia física, como también los mensajes de correo electrónico, constituyen una forma de comunicación privada constitucionalmente protegida. En consecuencia, se requiere una adecuación normativa que, mediante texto expreso, eleve las exigencias para la procedencia de la medida investigativa de incautación de correos, aplicada a los correos electrónicos y otros mensajes almacenados.

En ausencia de tal adecuación normativa, se recomienda:

- Para los solicitantes de la medida de incautación de correo:
    - En las solicitudes de autorización para la incautación de servidores y equipos que contienen correos electrónicos, cumplir con las mismas exigencias que las interceptaciones de comunicaciones en general.
    - Presentar separadamente las solicitudes de interceptación de comunicaciones en tránsito de la incautación de registros de comunicaciones y el acceso a información o correspondencia almacenada en servidores remotos o locales.
- Para las autoridades judiciales receptoras de solicitudes de autorización de incautación de correo:
    - Verificar que las solicitudes de autorización para la incautación de servidores y equipos que contienen correos electrónicos cumplan con las mismas exigencias que las interceptaciones de comunicaciones en general.
    - En particular, verificar que los antecedentes presentados por el solicitante sean tales que la medida constituya una restricción lícita de la inviolabilidad de las comunicaciones, a fin de prevenir la nulidad del juicio por haberse infringido sustancialmente derechos y garantías constitucionales.

Se requiere claridad normativa respecto a que la facultad de interceptar comunicaciones abarca solo aquella información que se encuentre en ruta de intercambio, y no abarca en caso alguno el acceso a información almacenada en servidores remotos o locales, o en dispositivos de cualquier naturaleza, si dicho acceso no ha sido específicamente autorizado junto con la interceptación de comunicaciones.

c. Solicitud de datos de comunicación (metadatos)

El acceso por las autoridades competentes a los datos de comunicación conservados debe supeditarse a un control judicial previo, cuya decisión tenga por objeto un control sustan-

tivo a fin de limitar el acceso a los datos y su utilización a lo estrictamente necesario para alcanzar el objetivo establecido en la ley invocada, en los términos señalados en la sección de reglas generales.

El reconocimiento expreso por la ley del carácter de dato personal de los metadatos, al que nos referimos más abajo, debe ir acompañado del cambio de prácticas por parte de las policías y su forma de vinculación con las empresas de comunicaciones, que por sus funciones o por mandato legal almacenan datos de comunicaciones. En particular, debe relevarse el carácter ilícito, sujeto a responsabilidades legales, del acceso a los registros de metadatos por personas no autorizadas y de la entrega de esos registros a terceros sin autorización judicial dentro de un procedimiento legalmente tramitado.

La investigación de campo que deriva en el presente documento reveló que son frecuentes los casos en que elementos de las policías recurren a sus relaciones personales y a sus privilegios de autoridad para obtener acceso a este tipo de información. Aunque la información recabada muestra una creciente resistencia de parte de las empresas a este tipo de prácticas, el hecho que elementos específicos de las fuerzas policiales recurran, o intenten recurrir a ellas, da cuenta de la ausencia de estándares claros y de consecuencias legales y administrativas para quienes los infrinjan. Por tanto, recomendamos adicional claridad normativa a este respecto ya sea por vía legal o reglamentaria.

La modificación normativa debiera reflejar las recomendaciones siguientes:

- La solicitud de entrega de metadatos debe estar asociada a la investigación de hechos constitutivos de delitos graves, y cumplir con los requisitos propios de la solicitud de interceptación de comunicaciones.
- Establecer obligaciones para las empresa de comunicaciones de contar con protocolos claros y públicos para la entrega de información a la autoridad, que haga explícita la necesidad de una orden judicial para hacer procedente la entrega. Junto a la obligación de informar a los usuarios de tales políticas y de las medidas técnicas y organizativas para prevenir el acceso no autorizado y la entrega no autorizada a terceros, así como las medidas de seguridad para la conservación de los datos y sus protocolos de eliminación transcurrido el plazo legal mínimo.

d. Incautación y análisis de equipos

Se requiere claridad normativa respecto a que la facultad de interceptar comunicaciones abarca solo aquella información que se encuentre en ruta de intercambio, y no abarca en caso alguno el acceso o incautación de dispositivos de cualquier naturaleza que de origen a tal comunicación o en que se puedan encontrar respaldos de las comunicaciones desarrolladas, si dicha incautación no ha sido específicamente autorizada junto con la interceptación de comunicaciones.

A la incautación de equipos se aplica todo lo indicado en la sección de reglas generales, en cuanto se trata de una medida de vigilancia en el marco de un proceso de investigación criminal. En particular, tratándose de dispositivos informáticos con capacidad de conexión a internet, incluyendo computadores portátiles, tabletas y teléfonos inteligentes, la aplicación de las reglas generales para la incautación de objetos y documentos (artículo 217 del Código Procesal Penal) no es suficiente para hacer examen de la totalidad de la información contenida en ellos.

El potencial de afectación de derechos fundamentales por el acceso no autorizado es colosal, por lo que es crítico que el sistema normativo entregue salvaguardas suficientes. Se trata de dispositivos contenedores de documentos, listas de contactos, comunicaciones orales, escritas y audiovisuales, datos sobre las comunicaciones, registros de movimientos, mensajes de correo electrónico, actividad privada en múltiples plataformas de internet y mucho más, referido tanto a la usuaria regular del dispositivo como a otras personas no necesariamente involucradas en investigación alguna. Por tanto, el acceso lícito a tales contenidos para su eventual utilización en la investigación debe estar sujeto al estricto cumplimiento de los estándares propios de la interceptación de comunicaciones privadas.

En la investigación de campo conducida por Derechos Digitales, diversos actores manifestaron preocupación por la elusión de la autorización judicial previa, en referencia a los dispositivos electrónicos con conexión a internet, mediante la entrega voluntaria de las personas propietarias o usuarias regulares de los dispositivos. Si bien esa entrega voluntaria es autorizada dentro de la legislación, en el caso de estos dispositivos, tal acto de entrega puede significar una disposición del derecho a la protección de la vida privada, de la inviolabilidad de las comunicaciones y del derecho a defensa, sin una intermediación judicial, y en atención a las circunstancias materiales de solicitud por parte de una autoridad policial o de persecución penal. La misma objeción es aplicable a cualquier acto de la autoridad consistente en coacción o solicitud, sin intermediación judicial, de desbloqueo, descifrado o superación de barreras técnicas de acceso al contenido de los dispositivos por parte de sus propietarias o usuarias.

En consecuencia, se recomienda:

- Extender requisitos propios de la interceptación de comunicaciones privadas para el acceso a tal información, manteniendo la práctica de solicitud de autorizaciones separadas para la obtención de aparatos electrónicos y para el acceso a su contenido.
- Prohibir el uso de herramientas de acceso forzado y de explotación de brechas de seguridad. Prohibir la entrega forzada de llaves, contraseñas o códigos de acceso o descifrado de información. Producir y publicar protocolos de acción en el sentido de estas recomendaciones.
- Exigir a las policías la entrega de información detallada sobre las técnicas de obtención de información de dispositivos electrónicos, y verificar que ellas no comprometan la seguridad ni la integridad del dispositivo o de los datos contenidos en él.
- Exigir a las policías la mantención y cumplimiento de medidas técnicas y organiza-

tivas de resguardo de los dispositivos en su custodia, de seguridad de la información contenida en ellos, y de limitaciones en acceso a la misma, incluida la eventual destrucción de cualquier copia o respaldo. Exigir a las policías la más pronta restitución posible de los bienes electrónicos.
- Exigir a los órganos de persecución medidas de transparencia con las personas afectadas por el examen de dispositivos electrónicos, afines a las recomendadas para la interceptación de comunicaciones, para el ejercicio de sus derechos, incluido su derecho a defensa.
- Terminar la práctica del uso de las reglas de incautación de objetos y documentos para la obtención de acceso a dispositivos electrónicos y a sus contenidos; en particular, la solicitud de entrega voluntaria de teléfonos inteligentes sin asesoría legal ni intervención judicial.

e. Uso de software malicioso o hacking para vigilancia

Se requiere claridad normativa respecto a que la facultad de interceptar comunicaciones o acceder a información almacenada en dispositivos, servidores locales o remotos, o a bases de datos comunicacionales legalmente almacenados, no autoriza la utilización por parte de las policías de software malicioso (*malware*) o técnicas de *hacking*. Recomendamos la incorporación expresa de prohibición de uso de herramientas maliciosas en la obtención de información desde sistemas, dispositivos y redes informáticas.

Pese a la evidente insuficiencia y desactualización de la ley de Delitos Informáticos (que deberá ser actualizada por la suscripción del Convenio de Budapest), el uso de software malicioso o técnicas de hacking por parte de las policías constituye hoy un ilícito informático. Consideramos pertinente que en la actualización de la ley se mantenga tal tipificación, y se consideren sanciones agravadas expresas al uso no autorizado de este tipo de herramientas por las policías.

2. Recomendaciones dirigidas a las funciones de inteligencia

i. Reglas generales

La regulación de las actividades de inteligencia en Chile, fundamentalmente contenida en la Ley Nº 19.974 sobre el Sistema de Inteligencia del Estado, padece de falencias significativas en razón de la amplitud del margen de acción para los órganos de inteligencia, que contrasta con la opacidad propia de esas mismas actividades. En lo referido al ejercicio de su capacidad de vigilancia, el sistema nacional de inteligencia requiere modificaciones sustantivas, que incluyan:

- Una mejor delimitación de los órganos con la capacidad de presentar solicitudes de autorización para actividades de vigilancia. Se requiere mayor claridad normativa respecto de los controles internos que permiten a cada una de las direcciones de inteligencia reconocidas en la ley solicitar el despliegue de medidas especiales de

obtención de información. En particular, la participación de altos mandos de las instituciones, como también de autoridades civiles, que validen de manera fundada la necesidad de tales medidas.

- Un mejor nivel de control por parte de las autoridades judiciales que autorizan las medidas especiales de obtención de información. Se requiere claridad normativa respecto del nivel de escrutinio exigido a las autoridades judiciales para hacer procedentes las medidas especiales, incluyendo la justificación completa de las resoluciones con ponderación de los derechos afectados, eventualmente considerar incluir la participación de un defensor público como representante de la ciudadanía como contraparte de los solicitantes. Se requiere claridad normativa respecto de la necesidad de que las autoridades judiciales conserven, bajo reserva, copias de los expedientes sobre los cuales resuelven las solicitudes de autorización de medidas especiales.
- Una separación completa de las funciones de inteligencia y de las de investigación criminal. Si bien ambas funciones no están hoy legalmente autorizadas para el intercambio de información, se requiere mayor claridad normativa sobre la improcedencia de utilizar información obtenida por los órganos de inteligencia dentro de procesos de investigación criminal, salvo excepciones calificadas legalmente y previa autorización judicial.
- Un mejor nivel de control externo y democrático de las actividades de vigilancia. En el caso de la Comisión de Inteligencia de la Cámara de Diputados, las sesiones deben ser registradas y mantenerse tales registros bajo reserva por cierto período de tiempo, después del cual pueda desclasificarse.
- Un mayor nivel de transparencia activa respecto de las actividades de inteligencia desplegada y sus resultados, con un nivel de detalle equilibrado con la necesidad de secreto para la consecución de sus fines institucionales, tales como informes detallados por categoría de operaciones que sean entregados bajo reserva a la Comisión de Inteligencia de la Cámara de Diputados.

ii. Reglas sobre vigilancia

Las normas que autorizan el uso de medidas especiales de obtención de información en el ámbito de la inteligencia son notoriamente amplias, dando un rango de acción que conlleva un impacto más intenso en los derechos de las personas bajo observación del aparato estatal de inteligencia. Por lo mismo, su uso debe ser restringido a casos altamente calificados, cuidadosamente analizados en su mérito fáctico y jurídico, en su impacto y en su viabilidad tecnológica:

- Deben precisarse las formas de obtención de información mediante procedimientos especiales. Se requiere claridad normativa respecto de los mecanismos que permiten materializar los procedimientos especiales de obtención de información. En particular, el ajuste a derecho del uso de herramientas de intervención de equipos o sistemas que exploten vulnerabilidades técnicas, y que por tanto puedan producir perjuicio o alteraciones en la integridad de la evidencia.

- Deben precisarse las consideraciones de ponderación de intereses y de protección de derechos fundamentales que debieran limitar el despliegue y uso de herramientas intrusivas. Se requiere claridad normativa respecto de la importancia crítica de los principios de legalidad, necesidad, idoneidad y proporcionalidad ya relevados a propósito de la vigilancia en el ámbito procesal penal.
- Deben precisarse las hipótesis de circunstancias de procedencia de uso de procedimientos especiales de obtención de información, a fin de prevenir un uso abusivo o arbitrario de técnicas de vigilancia e intrusión. Se requiere claridad normativa, a través de protocolos claros, celosamente seguidos, y sujetos a supervigilancia orgánica externa (no necesariamente pública), a fin de verificar que existe uniformidad de criterio para la ejecución de vigilancia altamente intrusiva.
- En el caso excepcional de ser autorizados por ley, debe garantizarse la existencia de registros que identifiquen a los funcionarios capacitados y autorizados para utilizar software malicioso o técnicas de hacking como herramientas de vigilancia, así como a la cadena de custodia respecto del proceso de selección de objetivos, operación del sistema y procesamiento de inteligencia obtenida a través de dichas herramientas.

3. Recomendaciones dirigidas a las funciones de prevención

i. Tecnología de televigilancia en espacios públicos

Parece útil contar con un marco normativo general que sistematice el uso de la televigilancia para distintas funciones (tránsito, seguridad pública, fiscalización medio ambiental, entre otros fines), ya que todos esos usos de vigilancia desarrollados en espacios públicos comprometen en algún grado el ejercicio de derechos fundamentales. Esta obligación solo puede satisfacerse adecuadamente a través de la dictación de una ley, que conforme se ha explicado bajo el principio de legalidad, es el instrumento normativo exclusivo cuando se trata de ponderar la afectación de derechos fundamentales.

Si bien a *priori* no existe una razón para considerar que la técnica legislativa de agrupar en un solo instrumento la regulación completa de sistemas de televigilancia sea una mejor solución que regular ámbitos específicos, la proliferación de estatutos específicos puede conducir a resultados contradictorios en la aplicación de los estándares para cautelar una efectiva protección de todos los intereses implicados en el uso de estas categorías de tecnología de vigilancia.

La experiencia comparada anotada en la investigación que nutre las presentes recomendaciones muestra varios casos en que se regula de manera integral el uso de sistemas de televigilancia, aplicable tanto a entidades públicas como privadas, y que de tal forma se asegura que sin perjuicio de diferencias que puedan ser atendibles en relación al objetivo que persigue la televigilancia, en todos los casos se establezcan regulaciones que garanticen la menor afectación de derechos fundamentales por el sistema implicado, así como mecanismos adecuados de control efectivos y recursos adecuados para quienes vean sus derechos fundamentales afectados por la televigilancia.

Por otra parte, el avance tecnológico determina que hoy sea cada vez más frecuente que los sistemas de televigilancia utilicen drones y globos aerostáticos equipados con cámaras de alta resolución, que intensifican con sus capacidades técnicas los riesgos de afectación de derechos fundamentales de los sistemas de televigilancia estáticos. Lo anterior justificaría el diseño de una normativa de televigilancia que también abarcara en forma específica el uso de tales dispositivos, así como otros de similar naturaleza que se creen en el futuro.

El uso de televigilancia por las Fuerzas de Orden y Seguridad Pública con fines preventivos, constituye una intervención administrativa que puede encontrar su justificación en el mandato que le formula el artículo 101, inciso segundo, de la Constitución Política, como un procedimiento destinado a garantizar el orden público y la seguridad pública interior. Sin embargo, a la fecha no existe una autorización legal para el uso de tales tecnologías por parte de las policías que satisfaga el principio de legalidad, ni menos para las autoridades locales, que han comenzado a implementar sistemas de televigilancia masiva en sus territorios.

La doctrina anota que hasta hoy, por regla general, los Gobiernos Regionales, Provinciales y las Municipalidades, financian el establecimiento de sistemas de videovigilancia, entregándolos posteriormente en comodato a las diversas dependencias operativas de Carabineros de Chile para que los utilicen.[7] A pesar de la utilidad que se le atribuye a estos sistemas de videovigilancia, no existen a nivel nacional un estudio que demuestre (sic) sus efectos en los planes de seguridad que adopta Carabineros de Chile, limitándose en consecuencia a meras apreciaciones de los usuarios de dichos sistemas.[8]

Por otra parte, las recomendaciones formuladas por el Consejo para la Transparencia[9] además de insuficientes en su contenido, de cara a los principios propuestos más arriba, carecen de fuerza obligatoria y de mecanismos de control para asegurar su eficacia respecto de los sistemas de televigilancia que se implementen por Municipios.

Así las cosas, se requiere una legislación integral en materia de televigilancia que se haga cargo a lo menos de los siguientes aspectos, de cara a los principios propuestos más arriba:

- Indicar los fines legítimos del Estado, y que sean necesarios en una sociedad democrática, que pueden ser invocados para la implementación de un sistema de televigilancia en espacios públicos.
- Señalar en forma clara y taxativa qué entidades públicas se encuentran habilitadas a implementar sistemas de televigilancia en espacios públicos.
- Exigir que previo a la implementación del sistema de televigilancia en espacios pú-

---

7 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.

8 Ibid, p. 81.

9 Consejo para la Transparencia, Oficio N°2309, de 6 de marzo de 2017, que Formula recomendaciones respecto a la instalación de dispositivos de videovigilancia por parte de las municipalidades, conforme a las disposiciones de la Ley N°19.628.

blicos se realice un informe escrito de evaluación de impacto en el ejercicio de derechos fundamentales, con el fin de determinar si los beneficios de dicha implementación son suficientes para justificarla; y en tal caso, identificar formas de mitigar o evitar cualquier efecto adverso para los derechos identificados.
- Someter la adquisición y mantenimiento de tecnologías de televigilancia en espacios públicos a controles de transparencia.
- Instar al desarrollo de procedimientos participativos de la ciudadanía en el proceso de evaluación de implementación de sistemas de televigilancia en espacios públicos.
- Establecer la obligación de acompañar la implementación de sistema de televigilancia en espacios públicos o privados de avisos generales al público, y luego de avisos específicos que acompañen los sistemas, además de la publicación de una política de uso del sistema de televigilancia por el responsable de éste.
- Indicar el procedimiento a seguir para examinar, usar y almacenar los datos obtenidos por el sistema de televigilancia en espacios públicos o privados.
- Determinar quiénes pueden tener acceso a los datos, en qué circunstancias y a quiénes pueden ser comunicados, tanto en sistema de televigilancia en espacios públicos o privados.
- Establecer un procedimiento de acceso a la información y reclamo por parte de quienes sientan vulnerados sus derechos fundamentales por el uso de un sistema de vigilancia en espacios públicos o privados.
- Precisar el plazo y las circunstancias en las cuales los datos obtenidos por un sistema de vigilancia en espacios públicos o privados pueden o deben ser borrados o destruidos.
- Considerar un órgano de control externo, que vele por el ejercicio de los derechos de las personas y, en particular, por las restricciones de acumulación y tratamiento de datos personales, tanto respecto de sistema de televigilancia en espacios públicos o privados.
- Someter el uso de tecnologías de televigilancia en espacios públicos o privados a obligaciones de seguridad respecto de los datos obtenidos.

ii. Uso de técnicas de identificación o perfilamiento a través de biometría

Como se puso de manifiesto en la investigación que nutre las presentes recomendaciones, el dato biométrico es una categoría de dato sensible hasta hoy no expresamente recogida en la normativa nacional de protección de datos personales, que surge a través de un proceso de registro o codificación de aspectos materiales (el iris, la huella dactilar, el ADN, el rostro) o inmateriales (la manera de caminar o el patrón de la voz) del cuerpo humano.

El uso de tecnologías biométricas para la identificación o el perfilamiento plantea una serie de cuestionamientos relativos no solo al impacto de estas tecnologías sobre la libertad de expresión y de acción en espacios públicos, sino a la autonomía y a la identidad del individuo.

Sin perjuicio que el Proyecto de Ley que actualiza la normativa de protección de datos personales (Boletín Nº 11.144-07) aborda con mayor precisión las exigencias a las cuales debe

someterse la recolección y procesamiento de esta categoría de datos, a través de las presentes recomendaciones expresamos consideraciones de política pública que abordan aspectos que van más allá del mero reconocimiento del estatus legal de protección de los datos biométricos, y pretenden proveer una directriz para la toma de decisiones acerca de la implementación de este tipo de tecnología para la identificación o perfilamiento de las ciudadanas en diferentes contexto de interacción con el Estado.

El uso de tecnologías biométricas por agentes estatales para cumplir con sus finalidades públicas debiera someterse a criterios estrictos de necesidad, idoneidad y proporcionalidad, que provean justificación a su implementación dado el enorme potencial de afectación que tales tecnologías tienen en el ejercicio del derecho a la privacidad de las personas. Además del reconocimiento legal como categoría de dato sensible por parte de la legislación, la recolección y uso de datos biométricos debiera someterse a un estándar alto de controles internos (para su adopción) y externos (para fiscalización de su adecuado uso).

La implementación reciente o anuncio de uso de este tipo de tecnología de vigilancia en servicios tales como la entrega de alimentación por la Junta de Nacional de Auxilio Escolar y Becas (registro de huellas de menores de edad en situación de vulnerabilidad), la fiscalización de la evasión de la tarifa de transporte público (a través de reconocimiento facial de usuarios del Transantiago), y el ejercicio de función preventiva en materia de seguridad pública (cámaras con tecnología de reconocimiento facial en espacios públicos en La Comuna de Las Condes) son solo tres ejemplos que sirven para mostrar que la aplicación de estándares mínimos para la implementación de sistemas biométricos resulta urgente.

Siguiendo los principios propuestos más arriba, y teniendo en consideración las reglas propuestas por el Boletín Nº11.144-07, nuestras recomendaciones adicionales de regulación son las siguientes:

- Indicar en la ley los fines legítimos del Estado, necesarios en una sociedad democrática, que pueden ser invocados para la implementación de un sistema de identificación o perfilamiento biométrico.
- Señalar por ley qué entidades públicas se encuentran habilitadas a implementar sistemas de identificación o perfilamiento biométrico.
- Exigir que previo a la implementación del sistema de identificación o perfilamiento biométrico se realice un informe escrito de evaluación de impacto en el ejercicio de derechos fundamentales, con el fin de determinar si los beneficios de dicha implementación son suficientes para justificarla; y en tal caso, identificar formas de mitigar o evitar cualquier efecto adverso para los derechos identificados. La necesidad e idoneidad de la implementación de este tipo de tecnología debe ser acreditada por el Estado. La mera disponibilidad de la tecnología a un costo relativamente bajo no es suficiente para justificar el uso de la tecnología.
- Someter la adquisición y mantenimiento de tecnologías de identificación o perfilamiento biométrico a obligaciones de transparencia activa y controles de rendición de cuentas.

- Establecer la obligación de acompañar la implementación de sistema de identificación o perfilamiento biométrico de la publicación de una política de uso del sistema por parte de su responsable.
- Indicar el procedimiento a seguir para examinar, usar y almacenar los datos obtenidos por sistema de identificación o perfilamiento biométrico.
- Determinar quiénes pueden tener acceso a los datos, en qué circunstancias y a quiénes pueden ser comunicados, tanto en sistema identificación o perfilamiento biométrico.
- Establecer un procedimiento de acceso a la información y reclamo por parte de quienes sientan vulnerados sus derechos fundamentales por el uso de un sistema de identificación o perfilamiento biométrico.
- Precisar el plazo y las circunstancias en las cuales los datos obtenidos por un sistema de identificación o perfilamiento biométrico pueden o deben ser borrados o destruidos.
- Considerar un órgano de control externo, que vele por el ejercicio de los derechos de las personas y, en particular, por las restricciones de acumulación y tratamiento de datos personales, tanto respecto de sistema de identificación o perfilamiento biométrico.
- Someter el uso de sistemas de identificación o perfilamiento biométrico a obligaciones de seguridad respecto de los datos obtenidos.
- Ya que los datos biométricos crudos generalmente contienen una cantidad importante de información adicional no requerida, particularmente información relativa a la salud del individuo o los hábitos del individuo, en caso de autorizarse su recolección deben ordenarse medidas que reduzcan la posibilidad de extraer esa información adicional que no guarde relación con el fin legítimo invocado para la implementación del sistema.
- En el caso de sistemas de identificación biométricos para el acceso de servicios, proveer mecanismos alternativos de autentificación que se hagan cargo de situaciones en que por razones de edad, mutilaciones u otros fenómenos físicos, el sistema no sea capaz de identificar a una persona. Esto último resulta crítico pues en otros países se han registrado casos de muerte por la incapacidad del sistema para identificar a ancianos y niños destinatarios de servicios de alimentación o salud.

4. Recomendaciones dirigidas al control de las tecnologías de vigilancia

i. Transparencia en la adquisición de tecnologías de vigilancia

El potencial intrínseco de las tecnologías de vigilancia para violar los derechos humanos hace necesario que el Estado defina marcos legales claros y específicos de quiénes pueden realizar estas compras y bajo qué condiciones, así como asegurar mecanismos de fiscalización independiente, transparencia y rendición de cuentas a la ciudadanía.

Todas las ciudadanas deben ser capaces de monitorear las compras y contrataciones de servicios al respecto. Para ello debiera considerarse como regla general a incorporarse en la normativa de compras públicas que toda adquisición de tecnologías de vigilancia solo pueda realizarse por licitación pública.

La obligación de transparencia debe extenderse a la información oportuna sobre su adjudicación, dando prioridad al principio de máxima divulgación, y acotando a su mínima expresión la aplicación de las figuras del secreto.

Los criterios de selección de proveedores deben ajustarse a un estándar de probidad y compromiso irrestricto con los derechos humanos en el país o en otros Estados: las empresas no deben presentar antecedentes de corrupción previa ni deben estar relacionadas -directa o indirectamente a través de sus intermediarios- en venta de tecnología de vigilancia que haya sido utilizada para violar los principios democráticos, los derechos humanos, en particular la privacidad, la libertad de expresión y de reunión o asociación.

Resulta deseable establecer por vía reglamentaria un código de conducta que sirva modelo para los responsables de la selección y contratación de tecnologías de vigilancia, quienes además debieran someterse a capacitación específica en materia de tecnología y respeto de derechos humanos.

ii. Protección de la ciberseguridad

Episodios recientes de vulneración de la seguridad de sistemas informáticos de entidades financieras privadas y de entidades públicas han puesto de manifiesto para la ciudadanía el rol fundamental de la ciberseguridad, en una era en que los servicios digitales y los datos que se generan a partir de estos se encuentran a merced de las vulnerabilidades técnicas de los sistemas que permiten su funcionamiento.

Si lo anterior resulta efectivo para toda clase de servicios en general, con mayor razón lo es cuando se trata de tecnologías de vigilancia implementadas por actores públicos o privados. Sin perjuicio de las mejoras que en este sentido introduce la normativa propuesta por el Boletín Nº 11.144-07 y de la directrices provistas por la Política Nacional de Ciberseguridad, estimamos que la protección de los datos recogidos por sistemas de vigilancia legalmente implementados (según los estándares y recomendaciones normativas expresados en los demás apartados de esta propuesta) requiere de la imposición de obligaciones para los controladores de tales sistemas que abarquen de manera específica al menos los siguientes aspectos:

- Establecer medidas que cautelen la integridad de los datos, y la protección de la seguridad de los sistemas que permiten su captura.
- Implementar las medidas técnicas y organizativas apropiadas para que los datos solo puedan ser accedidos por personal especialmente autorizado.
- Proteger a los datos, mediante las medidas técnicas y organizativas apropiadas, contra la destrucción accidental o ilegal por terceros, la pérdida o alteración accidental, la retención ilegal y el procesamiento, acceso o divulgación no autorizada o ilegal por terceros.

iii. Limitación a la recolección y retención de datos de comunicación

Los datos de comunicación o metadatos pueden dar a conocer aspectos altamente íntimos de las personas, es por ello que su retención en forma masiva no debe ser exigida por ley. Si bien hoy los datos de comunicación satisfacen la definición de datos personales contenida en la Ley de Protección de Datos Personales, en cuanto a la información que son capaces de aportar sobre un sujeto identificado o identificable, en innumerables ocasiones las prácticas de las autoridades y de los prestadores de servicios de comunicaciones fallan en reconocer dicho estatus a los metadatos. Con lo cual, se hace imperativo que el marco normativo provea un reconocimiento expreso del estatus de los datos de comunicación.

El acceso y utilización de datos de comunicación, en casos individuales, solo debieran ser exigidos en forma excepcional y por ley, cumpliendo con los exámenes de necesidad, idoneidad y proporcionalidad en las disposiciones que así lo establezcan, para proteger un interés legítimo en una sociedad democrática.

Deben establecerse criterios objetivos que permitan delimitar el acceso de las autoridades competentes a los datos de comunicación y su utilización posterior con fines de prevención, detección o enjuiciamiento de delitos que puedan considerarse suficientemente graves para justificar tal injerencia en otros derechos fundamentales.

Cumplido lo anterior, mediante ley es posible ordenar que categorías específicas de datos de comunicación (que satisfagan el examen de necesidad, idoneidad y proporcionalidad) se conserven durante un plazo limitado expresado en la ley, y en la cual se consignen además las obligaciones respecto de la conservación de tales datos, los mecanismos de acceso a los mismos, los sujetos autorizados a acceder a ellos, la forma de transferencia de los mismos y los plazos y condiciones para su destrucción.

El acceso por las autoridades competentes a los datos de comunicación conservados debe supeditarse a un control judicial previo, cuya decisión tenga por objeto un control sustantivo a fin de limitar el acceso a los datos y su utilización a lo estrictamente necesario para alcanzar el objetivo establecido en la ley invocada.

Las normas vigentes de retención de datos (artículo 222 CPP y Decreto 142-2005) no satisfacen los estándares aquí señalados, en cuanto no consignan un plazo limitado de conservación, sino solo un mínimo, ni son suficientemente detallados en los demás aspectos recién expresados.

Sin perjuicio de lo dispuesto en la normativa de Protección de Datos Personales, la normativa de telecomunicaciones debiera hacerse cargo de proveer reglas e incentivos para limitar la retención masiva de datos de comunicación en forma voluntaria por parte de los prestadores de servicios de comunicación. Ello en atención al riesgo de afectación de derechos fundamentales que el uso o la filtración de tales datos puede generar. Como parte de los objetivos

de protección al consumidor cubiertos por la normativa de telecomunicaciones, la autoridad respectiva debiera contar con potestades para fiscalizar y sancionar el incumplimiento de las limitaciones que en este sentido sean impuestas.

En tal sentido, recomendamos que la normativa de telecomunicaciones establezca obligaciones para los prestadores de servicios de comunicaciones que abarquen al menos los aspectos de ciberseguridad señalados en el apartado anterior.

V. Reflexiones finales

Las recomendaciones aquí propuestas no pretenden agotar todos los espacios donde las reformas normativas son necesarias, ni preterir las discusiones ya iniciadas a propósito de la reforma a la regulación de datos personales y de ciberdelitos. No obstante, esperamos que los principios orientadores propuestos, contribuyan a que esas discusiones tengan el pleno respeto por las personas y sus derechos fundamentales como su norte.

Es nuestra expectativa que, estas propuestas motiven la acción de los actores del Estado, y que estos se abran a un diálogo sobre las condiciones sistémicas para asegurar el pleno ejercicio de derechos fundamentales en el uso de las tecnologías de comunicación. Ello, para dar inicio a los cambios normativos que estimamos necesarios y urgentes para habilitar las condiciones de ejercicio de derechos más allá del control de la vigilancia.

Pero además, para permitir que los actores del sistema integren visiones protectoras de derechos en su actuar cotidiano. Tanto en el diseño de las normas habilitantes del sistema, pero también como recurso interpretativo donde tales normas no existen o no son suficientemente claras hoy, ya que la protección de los derechos fundamentales dictada por la Constitución y los tratados internacionales de derechos humanos ratificados por Chile, también es ley.


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina