Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Chile

Por Valentina Hernández, Juan Carlos Lara
con los aportes de Katitza Rodríguez

Julio 2016

ELECTRONIC FRONTIER FOUNDATION

DERECHOS DIGITALES América Latina

Valentina Hernández es investigadora de la ONG Derechos Digitales y egresada de la carrera de derecho de la Universidad de Chile. Juan Carlos Lara es director de investigación y políticas públicas de la ONG Derechos Digitales y abogado egresado de la Universidad de Chile.

Informe preparado en alianza con la Electronic Frontier Foundation (EFF). Agradecemos los aportes de Katitza Rodríguez, Directora Internacional de Derechos Humanos por la revisión sustantiva del informe, Kim Carlson y David Bogado de EFF por la corrección de estilo y formato.

El presente reporte forma parte del proyecto regional "Vigilancia y Derechos Humanos" llevado a cabo en ocho países de América Latina por EFF, una organización internacional sin fines de lucro que desde 1990 defiende la libertad de expresión y la privacidad en el entorno digital.

Derechos Digitales es una organización de alcance latinoamericano, independiente y sin fines de lucro, fundada en 2005 y que tiene como objetivo fundamental el desarrollo, la defensa y la promoción de los derechos humanos en el entorno digital. El trabajo de la organización se concentra en tres ejes fundamentales: Libertad de expresión, privacidad y datos personales y derechos de autor y acceso al conocimiento.

Índice de contenido

Introducción

En la sociedad actual las tecnologías de comunicación juegan un rol fundamental, generando amplios beneficios y suponiendo una ayuda considerable al quehacer humano. No obstante, no todo es positivo. Como ha señalado la Oficina del Alto Comisionado de Naciones Unidas para los Derechos Humanos en 2014, así como éstas tecnologías facilitan la vida y están al alcance de todos, igualmente se encuentran a disposición de los gobiernos, para los cuales conducir actividades de vigilancia de la población nunca fue más sencillo, barato y eficiente.[1]

Ante esta constante posibilidad de vigilancia del Estado, usualmente justificado[2] bajo argumentos de seguridad nacional, resulta necesario poner atención sobre los derechos fundamentales que pueden verse vulnerados y los controles necesarios para evitar excesos. Especialmente cuando se trata de derechos que están garantizados y reconocidos de forma explícita en la Constitución chilena como también en los instrumentos tradicionales ratificados por el Estado chileno.

Dentro de esta gama de derechos afectados, los que son especialmente vulnerables, a primera vista, son el derecho a la privacidad, al debido proceso y a la libertad de expresión. Pero no se trata de los únicos, pudiendo extenderse a libertad de reunión y de asociación. Es por ello que una legislación robusta y concordante es algo fundamental ante este panorama, la cual pueda proteger a la persona ante tales formas de injerencia a su vida privada y de transgresión a estos otros derechos.

No obstante, en Chile la realidad dista de lo óptimo. Disposiciones de carácter muy general y leyes anquilosadas, que no se adecuan efectivamente a la realidad actual y al vertiginoso desarrollo tecnológico es uno de los grandes problemas. Además la normativa protectora se encuentra dispersa, repartida entre la Constitución, leyes y regulación administrativa de difícil seguimiento y control. Esta hecho hace que la tutela en favor del afectado por la actividad de vigilancia esté esparcida y, por ende, sea menos efectiva que la mayormente cohesionada regulación que autoriza vigilar a parte de la población.

En Chile no estamos ajenos a la vigilancia en el entorno digital. En los últimos años, han salido a la luz casos cuyo elemento en común es la recopilación de información de comunicaciones en línea por parte de organismos públicos. Dicha actividad invasiva se viene realizando a través de conductos distanciados del derecho al debido proceso. Así, se han solicitado a adminstradores sin orden judicial las direcciones IP de usuarios que comentan en un determinado sitio web.[3] Asimismo, se acusó a un estudiante por supuestamente agredir a un carabinero en una protesta en Santiago en Mayo del 2014. La única evidencia

presentada por la unidad de Inteligencia de Carabineros consistió en capturar el material audiovisual donde se veía parcialmente el rostro de uno de los posibles agresores. Con esa imagen buscaron en los perfiles de la plataforma Facebook, usando técnicas de reconocimiento facial, hasta dar con la fotografía de alguien que se pareciera. El juez rechazó la evidencia, quien llamó a la Fiscalía a tener "más seriedad al llevar a cabo las indagatorias."[4] También ha habido un creciente número de demandas de datos sobre las empresas internacionales de Internet. Con respecto a estas solicitudes de cooperación con Estados Unidos, en 2011 hubo 47 casos, mientras que el 66 se registraron en 2012. Según el director adjunto de la Unidad de Cooperación Internacional y Extradición de la Fiscalía Nacional, "el aumento se debe a dos razones. difusión y explosión de Twitter como un medio de comunicación, y mejor en las relaciones con los EE.UU. Si no hubiéramos tenido respuesta favorable, habría un aumento, dijo al diario la Tercera".[5]

En el presente trabajo analizaremos el marco normativo sobre protección de derechos fundamentales ante la vigilancia gubernamental aplicable a Chile. Revisaremos las principales leyes chilenas que facultan a las autoridades a ejecutar actos de vigilancia en el entorno digital, específicamente, las propias del sistema de persecución penal y de la Agencia Nacional de Inteligencia (en adelante, ANI).

En base a tal análisis, examinaremos si la normativa nacional cumple con los estándares fijados en los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.[6] No se trata de un afán meramente académico o teórico. El cumplimiento de tales estándares es identificable como apego al marco de respeto de derechos fundamentales que ya es posible encontrar tanto en las normas constitucionales internas, como en los instrumentos internacionales de derechos humanos suscritos y ratificados por Chile. El cumplimiento de tales Principios, en consecuencia, equivale al respeto de las normas supralegales vigentes. Desde la perspectiva del respeto a los derechos fundamentales, ese respeto es plenamente exigible a la acción estatal.

En el presente trabajo se utiliza la definición de vigilancia de las comunicaciones dispuesta en el texto de los Principios anteriormente señalados: "monitorear, interceptar, recoger, analizar, usar, preservar, guardar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona, se derive o surja de ellas."[7]

Finalizaremos el presente informe enumerando recomendaciones al Estado chileno para una protección efectiva de los derechos fundamentales ante la vigilancia de las comunicaciones por parte de agentes o funcionarios del Estado, basándonos para ello en el diagnóstico realizado en los apartados previos.

1.
Marco Constitucional de Protección de los Derechos Afectados por las Actividades de Vigilancia Estatal de las Comunicaciones

Como se indicó en la introducción, las actividades de vigilancia estatal son capaces de afectar una serie de derechos fundamentales, tales como la privacidad, la libertad de expresión, la libertad de asociación y otros.

A continuación, revisaremos cómo están reconocidos en la carta fundamental de Chile y luego, su reconocimiento jurisprudencial en casos de vigilancia extensibles a la vigilancia de las comunicaciones. Asimismo, en virtud de la habilitación del artículo 5º de la Constitución,[8] se recurrirá a la Convención Americana sobre Derechos Humanos, plenamente aplicable como legislación nacional chilena de nivel supralegal.[9]

1.1 Privacidad

El artículo 19 Nº4 de la Constitución de 1980 asegura "el respeto y la protección a la vida privada" de la persona y de su familia. A continuación, en el artículo 19 Nº 5, se refiere a la "inviolabilidad del hogar y de toda forma de comunicación privada", dando nociones de intimidad en un sentido espacial. La garantía del artículo 19 Nº 4 utiliza el concepto de "vida privada" y no el de "privacidad". El concepto de vida privada, según los integrantes de la comisión encargada de su redacción, se encontraba más desarrollado en el lenguaje común. Había un reconocimiento por parte de la colectividad que se respetaba la vida privada y que "privacidad" era un término menos conocido, extraño a nuestro lenguaje.[10] Desde este punto de vista, si bien la Constitución chilena no regula un derecho a la "privacidad", aquellos intereses vinculados a ella sí están presentes en la normativa constitucional.

Así, parece existir una protección desglosada de la intimidad, con distintas consecuencias. A partir de la garantía de protección de la vida privada se ha esbozado la protección de las personas frente al tratamiento de sus datos personales, como veremos más adelante; sin embargo, hasta antes de la promulgación de la Ley 19.628, el tratamiento ilícito de los mismos era solamente impugnable mediante la acción constitucional (o "recurso") de protección. Si bien la Constitución recoge la idea de "vida privada" como bien jurídico digno de protección, no existe una definición en la regla constitucional ni en la ley de lo que debe entenderse por "vida privada", dejando como tarea a la jurisprudencia su delimitación.

Respecto de la protección de los datos personales, permanece sin consagración

constitucional directa como derecho independiente, y tampoco aparece entre los derechos vinculados a la vida privada.[11] Esta ausencia es llamativa, puesto que en el contexto Latinoamericano la mayoría de los países garantiza constitucionalmente a la protección de datos personales, siendo Chile una de las excepciones.[12]

No obstante, la jurisprudencia del Tribunal Constitucional desarrolla la protección de datos personales a partir de este derecho (vida privada), en casos específicos y sin el carácter de jurisprudencia generalmente vinculante.[13]

Lo anterior sin perjuicio de los intentos de reforma constitucional tendientes a disponer desde la carta fundamental resguardo a los datos personales.

En relación a otros aspectos, no existe hasta el momento un pronunciamiento del Tribunal Constitucional sobre vulneraciones a este derecho ocasionados por actividad de vigilancia de comunicaciones. Mayoritariamente, las leyes íntimamente relacionadas con la vigilancia contemplan dentro de sí mecanismos para el control del ejercicio de dicha actividad. Sin perjuicio de ello, como estudiaremos, es cuestionable si es que esos estándares y mecanismos legales responden a requerimientos constitucionales.

La Convención Americana sobre Derechos Humanos, en su artículo 11 sobre protección a la honra y a la dignidad, trata dentro del mismo en el numeral segundo al derecho a la privacidad. Señala que "nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación". Añade en el tercer numeral que toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

En 2009, la Corte Interamericana de Derechos Humanos se pronunció sobre un caso en el cual se interceptaron comunicaciones telefónicas entre miembros de una asociación de trabajadores rurales en la sentencia *Escher y otros v Brasil.* Allí, en el párrafo 114 este tribunal internacional se refirió a la aplicación del artículo 11 ya citado en relación a la actividad de vigilancia policial, indicando que:

> *"(...) El artículo 11 protege las conversaciones realizadas a través de las líneas telefónicas instaladas en las residencias particulares o en las oficinas, sea su contenido relacionado con asuntos privados del interlocutor, sea con el negocio o actividad profesional que desarrolla. De ese modo, el artículo 11 se aplica a las conversaciones telefónicas independientemente de su contenido e incluso, puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los*

> *interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones. En definitiva, la protección a la vida privada se concreta en el derecho a que sujetos distintos de los interlocutores no conozcan ilícitamente el contenido de las conversaciones telefónicas o de otros aspectos, como los ya mencionados, propios del proceso de comunicación."*[14]

Luego, en el párrafo que sigue hace énfasis en el riesgo que sufre hoy el derecho a la vida privada ante la fluidez informativa, dado las herramientas tecnológicas actualmente disponibles y su uso cada vez más frecuente. Ahonda en que estas interceptaciones y grabaciones de comunicaciones telefónicas no significa en caso alguno que las personas deben quedar desprotegidas ante el Estado o particulares, sino que, al contrario, este último debe adecuar a tiempos actuales las fórmulas tradicionales de protección a dicho derecho.[15]

De lo anterior se desprende que, el estándar del Sistema Interamericano ante vigilancia y privacidad comprende:

- El artículo 11.2 y 11.3 comprende dentro de la protección al derecho a la vida privada la tutela ante toda injerencia a este derecho, ya sea por el canal de comunicaciones que se trate, tanto telefónico, como correspondencia como medios de comunicaciones digitales.
- Abundando en eso, para entender adecuadamente este derecho, es necesario adecuarse a la tecnología vigente que pueda transgredirlo. Para ello, se solicita al Estado adecuar sus políticas y formas de protección al mismo, mandato contenido en el artículo 11.3 de la Convención.
- La actividad de vigilancia no solo lesiona el derecho a la privacidad en aquellos casos en que se registre el contenido mismo de la comunicación, sino también todo otro elemento de ese ejercicio comunicativo.
- Como se señaló en el caso *Tristán Donoso v Panamá* en el año 2009, este no es un derecho absoluto y, por lo tanto, puede ser restringido por los Estados siempre que las injerencias no sean abusivas o arbitrarias, es decir, tienen que estar previstas en ley, perseguir un fin legítimo y cumplir con los requisitos de idoneidad, necesidad y proporcionalidad.[16]
- En el mismo sentido que la Corte se manifestó la Relatoría Especial de Libertad de Expresión de la OEA en 2013 en la Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión.[17] En sus puntos 9 y 10, al referirse sobre la necesidad de limitar tales programas, reitera los requisitos que deben cumplir toda limitación al derecho a la privacidad ya enunciadas por la Corte Interamericana. Agrega que tal actividad vulneratoria de los derechos a la privacidad y libertad de expresión debe ser vigilada por un organismo de control independiente

y que en ella deben contarse con las garantías mínimas del debido proceso y supervisión judicial. Por otro lado, ejemplifica lo que sería una injerencia ilegítima a estos derechos, señalando los casos de persecución política contra periodistas y medios de comunicación independientes.

Dentro de este bloque, entonces, encontramos reconocimientos a nivel constitucional de aquello que la Constitución chilena denomina separadamente "vida privada" e "inviolabilidad de las comunicaciones privadas" y del hogar.

1.2 Libertad de Expresión, Libertad de Reunión y Derecho de Asociación

Las libertades vinculadas a la expresión están reconocidas por la Constitución chilena en el artículo 19 Nº 12, inciso primero, como la garantía constitucional sobre la "libertad de emitir opinión y la de informar, sin censura previa, en cualquier forma y por cualquier medio, sin perjuicio de responder de los delitos y abusos que se cometan en el ejercicio de estas libertades, en conformidad a la ley (...)".

Dentro de la doctrina nacional, Nogueira (2004), complementando la definición constitucional, ha entendido que este derecho engloba "la facultad de la persona para expresar de cualquier forma y por cualquier medio, sin censura previa, su universo moral, cognitivo y simbólico, vale decir, lo que tiene su origen y desarrollo en la esfera psíquica de la persona y es explicitado de propia voluntad (lo que cree, piensa, sabe o siente), a través de ideas y juicios de valor (sin que ellos constituyan en sí mismos vejaciones o insultos, innecesarios para expresar ideas), los que por su naturaleza, son subjetivos, pudiendo intercambiarlos y difundirlos. Tal derecho incluye el guardar silencio y no emitir opinión."[18]

De lo anterior, es posible desprender que el contenido esencial del derecho a la libertad de expresión bajo el derecho chileno está compuesto de los siguientes elementos:

- Emitir opinión, sin autorización ni censura previa.
- Libertad de informarse,
- Derecho a recibir información (incluyéndose aquí mismo a la información pública).
- Límite a este derecho: el discurso de odio.[19]

El mismo Tribunal Constitucional ha asociado la evolución histórica[20] de este derecho al rechazo a la censura previa, y al pluralismo propio de una democracia sana. Así, en los primeros textos constitucionales, el derecho a la libertad de expresión presentaba una serie de limitaciones previas usualmente ligadas al respeto de la honra, de la moralidad y credo. Posteriormente, la Constitución de 1980, en su versión inicialmente vigente, vetaba a una serie de grupos políticos, configurando el llamado régimen de "democracia protegida".

La redacción actual del precepto que consagra este derecho, eliminó las altas restricciones al ejercicio del mismo y fundamenta la libertad de expresión en el pluralismo político (señalando que este comprende la libertad para elaborar ideas, el derecho a difundirlas y a organizarse para llevarlas a la práctica), además del derecho de asociación, como pilares de un régimen democrático.[21]

En efecto, en palabras del mismo Tribunal Constitucional, la libertad de expresión y el derecho de asociación se relacionan de la siguiente forma: "El derecho de asociación resguarda la facultad de las personas para juntarse en forma estable con el propósito de promover ciertos ideales compartidos. Si no hubiera libertad para formular, adherir y expresar tales ideales comunes, el derecho de asociación perdería su razón de ser.

Así, la libertad de expresión desempeña un papel fundamental en la sociedad democrática, pues permite el debate de ideas, el intercambio de puntos de vista, emitir y recibir mensajes, la libre crítica, la investigación científica y el debate especulativo, la creación artística, el diálogo sin restricción, censura ni temor, y la existencia de una opinión pública informada."[22]

En cuanto a la garantía constitucional sobre la libertad de reunión, incluyendo aquellas con fines de expresión, el artículo 19 Nº 13 de la Constitución Política asegura a todas las personas: "El derecho a reunirse pacíficamente sin permiso previo y sin armas. Las reuniones en las plazas, calles y demás lugares de uso público, se regirán por las disposiciones generales de policía".

La doctrina entiende, en consecuencia, que este derecho consiste en la "libertad que tienen las personas para congregarse accidental o transitoriamente con el objeto de comunicar un hecho, discutir cualquier asunto o manifestar algún sentimiento u opinión."[23] En este sentido, las manifestaciones públicas reciben reconocimiento tanto en su arista de reunión como en el contenido del discurso expresado.

A ello se suma el derecho de asociación, recogido en el artículo 19 Nº 15 de la Constitución chilena, como garantía sobre "el derecho de asociarse sin permiso previo". La doctrina nacional ha entendido a este como el derecho que comprende la facultad individual de unirse voluntaria y establemente con otros para la consecución de determinados fines –esto es, formar una asociación o adherirse a una ya existente sin permiso previo– (dimensión individual de la libertad de asociación) y la facultad de auto-gobierno de la misma asociación creada (dimensión colectiva).[24]

Es precisamente este deber de no interferencia lo que afecta tanto a la libertad de expresión como a la libertad de reunión y a la de asociación. En la primera este derecho se ejerce sin

censura previa, atribuyéndose la responsabilidad civil o penal, en caso que procedan, con posterioridad al acto y no filtrando antes el contenido. En los otros dos casos, importa que mientras se cumplan los requisitos legales y el grupo (reunido o asociado) no atente contra la moral, el orden público y la seguridad del Estado, este último no puede prohibir el nacimiento de una nueva organización. Estos derechos son relevantes por cuanto son el canal de expresión de ideas necesarias en una democracia pluralista.

Los programas de vigilancia desmedidos son capaces de afectar a todo este cúmulo de derechos. Si bien el Tribunal Constitucional de Chile no se ha pronunciado específicamente respecto a la vigilancia en torno a ellos, una actividad de este estilo que no cumpla con los requisitos de legalidad, necesidad y proporcionalidad, atenta directamente en contra de estos.

En el caso de la libertad de expresión, genera temor en quienes buscan manifestarse de ser perseguidos y silenciados por su pensamiento. Por otro lado, programas de vigilancia desproporcionados también tienen similar repercusión en los derechos de reunión y de asociación, generando una intromisión indirecta a la faceta individual del mismo: el hecho que el Estado pueda identificar quién participa en una manifestación pública, o quién se une o conforma una determinada asociación, puede ser un factor suficiente para no ejercitar estos derechos, minando el valor discursivo dentro de una democracia.

Casos concretos han sido verificados en los últimos años. En 2011, el Ministerio del Interior de Chile presentó un proyecto de ley para combatir los efectos negativos ocasionados por las fuertes protestas sociales estudiantiles. Dicho proyecto pretendía sancionar tanto la participación como la convocatoria a una marcha pública que derivara en disturbios o destrozos.[25] Al mismo tiempo el poder público admitía la revisión de la actividad y comentarios hechos por usuarios chilenos de redes sociales, en relación al desempeño y opinión que tenían estos sobre el gobierno[26], además de una licitación pública buscando un servicio de ubicación geográfica, monitoreo, análisis de propagación y almacenamiento en internet sobre la discusión en redes sociales.[27]

A mediados del 2015, se conocieron documentos que ligan a la Policía de Investigaciones de Chile (PDI) con el pago del sistema Galileo de la empresa italiana Hacking Team, el cual permite acceder a computadores de forma remota, rápida y secreta.[28] Se rechazó tal nexo en un inicio por parte de la PDI, recalcando la ilegalidad de dicha conducta de vigilancia y la necesidad de una orden judicial previa para poder realizar gestiones de aquella envergadura. Posteriormente la PDI confirmó la adquisición de este sistema,[29] pero el asunto no finalizó ahí. La filtración incluyó una serie de correos electrónicos donde quedó constancia que el jefe del Departamento de Monitoreo Telefónico indica que el uso de dicha herramienta es en apoyo de la recolección de las direcciones IP de los clientes y a la obtención de datos que no pueden acceder mediante orden judicial previa.[30]

2.
Normativa Legal que Permite Actividades de Vigilancia de Comunicaciones

2.1 Ley General de Telecomunicaciones

En Chile, la Ley General de Telecomunicaciones Nº 18.168 es la encargada de regir sobre toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos e informaciones de cualquier naturaleza, por línea física, radioelectricidad, medios ópticos u otros sistemas electromagnéticos, contemplando normas sobre interceptación, difusión y protección de usuarios. Apunta a regular las telecomunicaciones como servicio y a la relación entre los distintos operadores de ese sistema.[31]

Específicamente, el artículo 24 H de la Ley de Telecomunicaciones establece un listado de deberes a las concesionarias de servicio público que presten servicio a los proveedores de acceso a internet, y también a toda persona natural o jurídica que preste servicios comerciales de conectividad entre los usuarios o sus redes en internet. Dentro de estos deberes se encuentra el preservar la privacidad de los usuarios de la red.

Aparte de esta mención genérica, la Ley de Telecomunicaciones no contempla hipótesis que permitan realizar actividades de vigilancia sobre las telecomunicaciones. No obstante esta carencia, es preciso revisar dos reglamentos complementarios de la misma ley: el Reglamento de la Ley de Telecomunicaciones (2014) y el Reglamento sobre Interceptación y Grabación de Comunicaciones Telefónicas y otras Telecomunicaciones (2005).

El Reglamento de Servicios de Telecomunicaciones, Decreto Nº 18, de enero de 2014, es el llamado a especificar sobre la aplicación de las disposiciones de la Ley General de Telecomunicaciones. En materia de privacidad, y junto con la garantía constitucional de inviolabilidad de las comunicaciones privadas, la ley establece que las concesionarias de servicios de telecomunicaciones mantienen de forma principal la obligación de preservar la privacidad de los usuarios. Así, sanciona la interceptación o captación maliciosa o grave, sin la debida autorización, de cualquier tipo de señal que se emita a través de un servicio público, con penas restrictivas o privativas de reclusión y multa; las penas aumentan si existe difusión pública o privada del contenido de esas señales.

Complementando a la Ley en temas de vigilancia y privacidad, el Reglamento contiene dos artículos de especial relevancia. El primero de ellos, el artículo 24, que se refiere a los datos personales de suscriptores y usuarios de los servicios de telecomunicaciones en Chile. Esta

norma indica que tales datos solo podrán utilizarse en relación a los fines específicos asociados a la prestación del servicio. Además, deben someterse a lo dispuesto en la Ley sobre Protección de la Vida Privada (esto es, la Ley Nº 19.628, que solamente regula datos personales).

Acá se repite uno de los puntos claves de la ley que viene a complementar: la obligación de los Proveedores de Servicios de Internet (ISP en inglés) de proteger la privacidad de los usuarios del servicio de acceso a internet. Por tanto, ello no se hace únicamente mediante la prohibición de la interceptación de los servicios prestados, sino que igualmente evitando la filtración de datos que puedan afectar a la privacidad de las personas por parte de ellos mismos, actuando como partes de un contrato.

Vuelve sobre protección de la privacidad de los usuarios el artículo[32] 50º del Reglamento al señalar que los ISP procurarán preservar la privacidad y seguridad de los usuarios en la utilización del servicio de acceso a Internet. A diferencia de la norma anterior, se dirige a la privacidad en relación al uso mismo del servicio de Internet y, además, no es un mandato general a todo tipo de servicios de telecomunicaciones[33] sino únicamente para internet, pero que sigue la misma idea base.

El segundo reglamento, más relevante para fines del presente estudio, es el Decreto Nº 142 del Ministerio de Transporte y Telecomunicaciones, de septiembre de 2005. También se conoce como "Reglamento sobre Interceptación y Grabación de Comunicaciones Telefónicas y de otras formas de Comunicaciones". Su finalidad es regular el procedimiento que deberán seguir los prestadores de servicios de telecomunicaciones frente a los requerimientos judiciales para proceder a la interceptación y a la grabación de las comunicaciones sostenidas por los usuarios de servicios telefónicos y de todo tipo de telecomunicaciones en general.

Las medidas de intervención sobre las comunicaciones, habilitadas y reglamentadas específicamente en este último reglamento, se encuentran normadas en las reglas de persecución criminal que se examinan a continuación. El Decreto Nº 142 es la normativa que vino a complementar a la Ley de Telecomunicaciones ante las modificaciones legales realizadas en materia penal que comenzaron a exigir ciertas obligaciones de registro, y a autorizar diligencias intrusivas que la ley no contempla dada su antigüedad.

2.2 Reglas Especiales del Sistema Procesal Penal

El sistema procesal chileno, desde el punto de vista de la reglamentación de las medidas intrusivas de recolección de información, se encuentra dividido entre un sistema general aplicable a los delitos y crímenes comunes, y reglas especiales para materias sensibles.[34] Sobre esto último, trataremos de forma separada dos leyes de particular interés: la Ley Nº 18.314

que determina conductas terroristas y fija su penalidad (más conocida como la "Ley Antiterrorista") y la Ley Nº 20.000 que sanciona el tráfico ilícito de estupefacientes y sustancias psicotrópicas (usualmente llamada "Ley de Drogas").

En general, la regulación de la investigación y enjuiciamiento de los delitos, contenida en el Código Procesal Penal del año 2000, persigue un equilibrio de intereses entre la persecución penal y los derechos de los intervinientes en el juicio. En la regulación específica sobre las diligencias de investigación que puede ordenar el Ministerio Público (el órgano que dirige la investigación penal, conocido también como Fiscalía), el Código contempla una serie de medidas intrusivas regladas y armonizadas con los Principios de Legalidad, Necesidad y Proporcionalidad como fundamento de la procedencia de las actuaciones. Estas diligencias reguladas incluyen los exámenes corporales y médicos, la entrada y registro de lugares cerrados, la retención e incautación de correspondencia, la interceptación de telecomunicaciones, y la incautación de objetos y documentos.

Si bien se consideran una serie de medidas intrusivas en específico, como las diligencias ya citadas, el principio general sobre materia probatoria e intervención judicial previa se puede encontrar dentro de principios básicos informadores del sistema procesal penal chileno. Así, el artículo 9º del Código Procesal Penal, titulado "Autorización Judicial Previa", indica que "toda actuación del procedimiento que privare al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o lo restringiere o perturbare, requerirá de autorización judicial previa".

Por ello, todo tipo de diligencia probatoria que importe actividad de vigilancia por parte del Ministerio Público o las policías, que afecte los derechos fundamentales ya expresados, y sea que esté o no consagrada y regulada de forma especial en el Código, requiere de autorización por el Juez de Garantía competente. El estándar en Chile, al que debería ceñirse el juez, es el *test de proporcionalidad* entre la afectación a los derechos fundamentales del imputado y la medida solicitada.

En virtud de dicho test, el Juez deberá ponderar la idoneidad, necesidad y proporcionalidad en sentido estricto de esta medida en relación con sus fines, frente a la afectación de derechos que se puede producir. Si bien el artículo 9º no contempla específicamente este examen de proporcionalidad como estándar, ya en otras disposiciones es posible vislumbrar elementos de este. Por ejemplo, la medida de interceptación de comunicaciones telefónicas u otro tipo de telecomunicaciones exige que la pena asociada al delito investigado debe ser, como mínimo, de cinco años y un día de prisión para poder ser autorizada. Asimismo, esta diligencia contempla como requisito que la puesta en práctica de la misma sea imprescindible dentro de la investigación.

Independiente de este test de proporcionalidad que debería aplicarse al sopesar los derechos

del investigado con las ventajas y beneficios que puede producir tal intromisión en la investigación penal, cabe destacar que la normativa chilena referente a cada una de estas diligencias intrusivas cambia según sea la medida. Así, cada una de estas presenta requisitos y estándares diferentes, lo cual hace que la regulación sobre autorización de este tipo de providencias sea poco armónica y desigual.

Excepcionalmente, cuando la autorización judicial sea indispensable para el éxito de la diligencia, y que el éxito de la medida dependa del desconocimiento del afectado, no se dará a conocer al sujeto investigado.

Dada esta regla general, incluso si los órganos públicos (Fiscalía o policías) que participan del proceso penal desean ejecutar algún tipo de gestión probatoria que no está expresamente contemplada o regulada en el Código Procesal Penal, podrían en teoría realizarla si ello incide en la investigación, previa autorización del juez de garantía. El límite natural, como se ha explicado, se encuentra en la posibilidad de vulneración de derechos fundamentales del investigado.

El Código establece también las normas sobre el desarrollo del procedimiento penal. A propósito de los requerimientos de información con carácter secreto que solicite el Ministerio Público y los tribunales con competencia penal a otros órganos del Estado, establece que "se atenderá observando las prescripciones de la ley respectiva, si las hubiere, y, en caso contrario, adoptándose las precauciones que aseguraren que la información no será divulgada" (Artículo 19, inciso segundo); luego, entrega la decisión a la Corte Suprema si la autoridad establece que la publicidad pudiere afectar la seguridad nacional (inciso cuarto).

Sobre el secreto de las actuaciones de investigación, dentro de las cuales se podría encontrar información obtenida mediante actividad de vigilancia estatal, el Artículo 182 establece, durante la etapa de investigación, esas actuaciones serán secretas para los terceros ajenos al procedimiento. Solamente el imputado y los demás intervinientes en el proceso están facultados para examinar y obtener copias de los registros y documentos de la investigación. Se exceptúan, aquellas piezas o actuaciones precisamente identificadas que el fiscal determine que deben ser mantenidas en secreto respecto del imputado o de los demás intervinientes cuando sea requerido para la eficacia de la investigación y cuyo plazo no exceda los cuarenta días.

En este sentido, no es posible la declaración de secreto respecto de las actuaciones en que ha intervenido o ha tenido derecho a intervenir el imputado. Tampoco es posible la declaración de secreto respecto de las actuaciones en que participare el tribunal ni los informes de peritos respecto del imputado o su defensor. Los funcionarios que hubieren participado en la investigación o que tengan conocimiento de las actuaciones tienen la obligación de guardar secreto; en caso contrario, se constituye el delito de violación de secretos del Código Penal.

Los artículos 218, 219 y 220 del Código Procesal Penal se refieren a la retención e incautación de correspondencia. Si bien no se contiene a la correspondencia electrónica de forma expresa en el listado inicial de tipos de comunicaciones, al final del listado se señala "otros", tornando esta enumeración en una netamente ejemplar. Así, se indica que previa resolución fundada (tal y como funciona el sistema, apreciable desde el genérico artículo 9º), el Juez de Garantía puede autorizar la retención e incautación de la misma e incluso la copia de correspondencia y transmisiones, si de esa forma lo solicita el fiscal de la causa, además de aplicarse por analogía estas disposiciones procesales.

Además de autorización judicial previa y razonada en la cual permita la ejecución de la medida, el otro requisito que establece la ley apuntan a que las especiales circunstancias se presume que la correspondencia emana del investigado o que este es su destinatario. Se exige que se fundamente que es previsible que la retención e incautación de correspondencia será de utilidad en el marco de la investigación.

No obstante, sí existen menciones específicas sobre la correspondencia electrónica más adelante, específicamente al tratar la copia de las mismas, tanto en el artículo 218 como en el 219. La primera de estas disposiciones expresa que se podrá disponer la obtención de copias o respaldos de la correspondencia electrónica dirigida al imputado o emanada de éste. El fiscal deberá examinar la correspondencia o los envíos retenidos y conservará aquellos que tuvieren relación con el objeto de la investigación. En segundo lugar, en la norma que trata en particular el tema de las copias, se indica que el juez de garantía podrá autorizar, a petición del fiscal, que cualquier empresa de comunicaciones facilite copias de las comunicaciones transmitidas o recibidas por ellas.

2.2.1 Interceptación de Telecomunicaciones

En términos simples, entendiendo que una persona intercepta una comunicación si, en el curso de su transmisión, como resultado de su interferencia en el sistema de transferencia de esta o de un proceso de monitoreo de comunicaciones, parte o la totalidad del contenido de la misma se hace disponible a un tercero diferente del emisor o del destinatario de esta.[35]

La interceptación telefónica y de otras formas de telecomunicación se regula en el artículo 222 del Código Procesal Penal. En tal disposición se indica que en caso de existir fundadas sospechas, basadas en hechos determinados, que una persona hubiere cometido o participado en la preparación o comisión, o que ella preparare actualmente la comisión o participación en un hecho punible que mereciere pena de crimen (es decir, que la pena asignada al delito sea de, al menos, cinco años y un día de prisión), y la investigación lo hiciere imprescindible, el juez de garantía, a petición del Ministerio Público, podrá ordenar la interceptación y grabación de este tipo de comunicaciones.

El requisito de las "fundadas sospechas" se refiere a que derivado de las circunstancias específicas del caso y hechos concretos que merezcan pena de crimen, se pueda argumentar que existe la creencia que la persona investigada ha participado en la preparación o comisión del delito o que lo hará. Igualmente, se establece un requisito de necesidad para la procedencia de la medida: que la medida sea imprescindible para el curso de la investigación.

De este modo, para ser autorizada una interceptación de este tipo de telecomunicaciones legalmente se exige el cumplimiento de una prueba de proporcionalidad: necesidad (marcada por que sea imprescindible para la investigación), idoneidad (analizar las circunstancias y hechos del caso, además de la necesidad de la medida) y proporcionalidad en sentido estricto (que el delito investigado tenga asociado una pena de crimen, es decir, que el delito tenga aparejada una pena de, al menos, cinco años y un día a prisión).

Respecto a la implementación de esta medida, el mismo Ministerio Público ha delineado su forma de ejercicio mediante el Oficio FN 060/2014, de enero de 2014. En este documento, consta que el organismo persecutor contempla el uso de esta medida en la investigación de casos complejos: secuestro, homicidio, tráfico ilícito de drogas, lavado de dinero, determinados delitos económicos, corrupción pública, delitos sexuales y, en general, la investigación vinculada a determinadas agrupaciones o derechamente casos de criminalidad organizada.[36]

Posteriormente, se exponen los criterios generales de actuación a seguir por parte del Ministerio Público previamente a presentar la petición al juez de garantía en esos casos. En resumidas cuentas contempla los siguientes pasos:[37]

- En primer lugar, el o los fiscales a cargo de la investigación en la cual se quiera ejecutar esta medida intrusiva requerirán a la policía que corresponda que elabore un informe escrito que de cuenta del motivo que justifique la utilización de la interceptación.
- Luego, los fiscales evaluarán tanto la pertinencia como el alcance de la interceptación de comunicaciones (para lo cual ponderarán los antecedentes entregados por la policía y las circunstancias del caso que consten en la carpeta investigativa).
- En tercer lugar, los fiscales, en la solicitud que se hará al Juez de Garantía, deben indicar el alcance de la solicitud de interceptación que están requiriendo. Este punto es de suma relevancia, pues, citando textualmente el documento: "(...) para lo cual señalarán expresamente si sólo se solicita la interceptación de la voz o si, además, requieren que el tribunal autorice la obtención del tráfico de llamadas, la información proveniente de los sistemas de mensajería u otras formas de telecomunicación que sean posibles de interceptar, conforme a las capacidades técnicas de las operadoras". Como se puede apreciar, los fiscales no solo pueden solicitar el contenido mismo de la comunicación, sino también los datos de la

comunicación (metadatos)- asociados.

- Aprobado el requerimiento, los fiscales deberán revisar que la resolución judicial apruebe expresamente todo el contenido de la solicitud.
- Finalmente, los Fiscales Regionales evaluarán y solicitarán al Director de la unidad especializada el uso del Servicio de Respaldo de Telecomunicaciones.

Complementario a esta norma es el Reglamento sobre Interceptación y Grabación de Comunicaciones Telefónicas y de Otras Formas de Telecomunicación del Ministerio de Transportes y Telecomunicaciones del año 2005. El mismo establece directrices generales sobre interceptación de telecomunicaciones, tendientes a resguardar la privacidad y, al mismo tiempo, a facilitar el trabajo de las policías en la investigación criminal.

Tales interceptaciones requieren que se cumplan una serie de requisitos, así:

- No se podrán interceptar las comunicaciones entre el imputado y su abogado. Se exceptuan en los casos donde el Juez de Garantía lo ordenare, por estimar fundadamente que el abogado pudiere tener responsabilidad penal en los hechos investigados, sobre la base de antecedentes de los que dejará constancia en la respectiva resolución.
- La orden que dispusiere la interceptación y grabación deberá indicar circunstanciadamente el nombre y dirección del afectado por la medida y señalar la forma de la interceptación y la duración de la misma, que no podrá exceder de sesenta días.
- Las empresas telefónicas y de comunicaciones deberán dar cumplimiento a esta medida. Ellas deben proporcionar a los funcionarios encargados de la diligencia las facilidades necesarias para que se lleve a cabo con la oportunidad con que se requiera.

Respecto a la grabación, ella se trata en específico en el artículo 223 del Código Procesal Penal, tal disposición contempla que:

- La interceptación será registrada mediante su grabación magnetofónica u otros medios técnicos análogos que aseguraren la fidelidad del registro.
- La grabación será entregada directamente al Ministerio Público, quien la conservará bajo sello y cuidará que la misma no sea conocida por terceras personas. Cuando lo estimare conveniente, el ministerio público podrá disponer la transcripción escrita de la grabación, por un funcionario que actuará, en tal caso, como ministro de fe acerca de la fidelidad de aquélla. Sin perjuicio de ello, el Ministerio Público deberá conservar los originales de la grabación.
- Aquellas comunicaciones que fueren irrelevantes para el procedimiento serán entregadas, en su oportunidad, a las personas afectadas con la medida, y se destruirá

toda transcripción o copia de ellas por el Ministerio Público.

- Lo anterior no regirá respecto de aquellas grabaciones que contuvieren informaciones relevantes para otros procedimientos seguidos por hechos que pudieren constituir un delito que merezca pena de crimen. En ese caso se podrá hacer uso del material interceptado conforme a las normas precedentes.

Ya revisado el marco general sobre interceptación y registro del contenido obtenido de dicha actividad contemplado en el Código Procesal Penal, es preciso volver a dirigir la atención del lector hacia el Decreto 142 del Ministerio de Transporte y Telecomunicaciones; Subsecretaría de Telecomunicaciones de septiembre de 2005, también conocido como "Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de comunicaciones."

El reglamento, ya en su primer artículo, indica que su finalidad es regular el procedimiento que deberán seguir los prestadores de servicios de telecomunicaciones frente a los requerimientos judiciales para proceder a la interceptación y a la grabación de las comunicaciones sostenidas por sus usuarios.

Un caso ilustra el uso de estas capacidades, más allá de su uso en procedimientos judiciales. En abril de 2012 fue formalizada la investigación, contra el ex jefe de la Dirección de Inteligencia de Carabineros (Dipolcar), el mayor Gonzalo Alveal Antonucci, por supuestamente interceptar ilegalmente el celular de un efectivo policial y usar esas escuchas para obligar su alejamiento de la institución.[38]

Según la investigación, entre los meses de mayo y julio del año 2010, el entonces jefe de asuntos internos de la Dipolcar, habría ordenado la interceptación telefónica de dos números celulares de funcionarios de la misma institución, sin mediar orden judicial y en el contexto de una investigación policial.

Según lo entendió el Ministerio Público, esa información era utilizada para fines ajenos a la investigación en curso, por lo que el mayor Alveal Antonucci fue formalizado por los delitos de obstrucción a la investigación y grabación de comunicaciones privadas sin autorización judicial. La investigación llegó a término sin sentencia.

2.2.2 Vigilancia Masiva: Retención Obligatoria de Datos de Comunicación

El artículo 222 del Código Procesal Penal de Chile, a propósito de la colaboración ordenada entre empresas de telecomunicaciones y órganos de investigación criminal, establece que "los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus

abonados. La negativa o entorpecimiento a la práctica de la medida de interceptación y grabación será constitutiva del delito de desacato. Los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este inciso deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento".

El citado "Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de comunicaciones" establece en su artículo 6º las obligaciones de los prestadores de servicios de Internet de mantener información sobre las comunicaciones de sus usuarios. En consecuencia, los proveedores de acceso a Internet deben mantener: un listado actualizado de sus rangos autorizados de direcciones IP, y un registro de los números IP de las conexiones que realicen sus abonados, por un tiempo no inferior a un año.

La obligación de registro consiste básicamente en un sistema computacional que deja constancia automática de ciertas operaciones que realiza un usuario en Internet, información que es almacenada en los equipos e instalaciones del ISP; usualmente el registro consigna la dirección IP utilizada por el usuario –la cual es asignada por el ISP–, la hora de conexión y la hora de desconexión de la red. De esta manera, su procesamiento posterior permite localizar o identificar el computador desde el cual se realizó una determinada operación en Internet, funcionando de manera similar al sistema de control de llamadas que las compañías telefónicas utilizan para efectos de facturación.[39]

El Reglamento obliga a mantener esa información en carácter reservado, pero "a disposición del Ministerio Público y de toda otra institución que se encuentre facultada por ley para requerirlo", obviando así la autorización judicial. A su vez, no contempla una norma para la eliminación de esos datos. Si tomamos al número de dirección IP como una serie o conjunto numérico que identifica a un dispositivo en Internet que ha sido reconocido por sistemas jurídicos extranjeros, como el español, como dato personal,[40] deberán aplicarse las reglas generales en materia de protección de datos, establecidas en la Ley 19.628, incluyendo su posibilidad de eliminación.

Igualmente la sentencia de la Corte Interamericana de Derechos Humanos en el caso *Escher y otros v Brasil*, hace extensiva la protección a la vida privada que consta en el artículo 11 de la Convención Interamericana de Derechos Humanos. La Convención protege no solo al contenido mismo de las comunicaciones privadas, sino que amplia el resguardo a los metadatos. En otras palabras protege también los datos asociados a los procesos de comunicaciones.[41]

Con respecto a las interceptaciones y grabaciones decretadas, dispone en reglamento que los prestadores de servicios de telecomunicaciones darán cumplimiento a ellas en el plazo y la forma establecida en el oficio respectivo por el tribunal que conozca de la causa. Respecto de las reglas seguidas por las policías, al revisarse las leyes orgánicas tanto de la Policía de

Investigaciones[42] como de Carabineros de Chile,[43] no existen menciones al respecto.

2.2.3 Vigilancia Focalizada: Malware

A mediados del 2015, fue revelada a través de filtraciones y reportes de prensa la compra y posterior utilización del sistema "Phantom" —desarrollada por la empresa italiana Hacking Team— por parte de la Policía de Investigaciones de Chile. Dentro de las opciones que da a quien lo utiliza están rastrear teléfonos mediante GPS, interceptar y recolectar mensajes de texto, correos electrónicos e historial de llamadas, grabar llamadas telefónicas, entre otros.[44] Si bien aún no se sabe de algún caso en específico en el cual este software haya sido utilizado, este órgano auxiliar de la investigación criminal pretende, al menos, ejecutarlo en delitos adscritos a las leyes sobre conductas terroristas y sobre tráfico de drogas.

En efecto, la misma PDI[45] indicó que la adquisición de "Phantom" viene a colaborar en el mejoramiento de capacidades técnicas la investigación del crimen organizado y de las redes internacionales, considerando que tales grupos criminales cuentan con amplios recursos, tanto financieros como técnicos.

No obstante la peligrosidad de aquellos ilícitos y las mayores concesiones que permiten estas leyes punitivas especiales, el requisito previo de necesidad de orden judicial para poder realizar actividades investigativas vulneratorias de derechos y libertades fundamentales sigue siendo aplicable. Según la PDI, se cumplieron las disposiciones propias del ámbito de las compras públicas, sin referirse más al tema ni transparentado más detalles al respecto, indicando que otorgar mayor información comprometía la seguridad nacional.

Las filtraciones de Wikileaks citadas anteriormente indican que este malware se usaría para obtener datos a los cuales normalmente no puede acceder con orden judicial. Esto es de suma gravedad, pues la intervención judicial es el momento en el cual se realiza el test de proporcionalidad entre el fin probatorio buscado y la vulneración a derechos del investigado. Según reportes, "Phantom" es altamente intrusivo y las garantías no deben ignorarse.

La Comisión de Control de Inteligencia de la Cámara de Diputados citó tanto a los directores de la PDI y la ANI a explicar la compra de este software. Si bien no es posible encontrar registros de dicha sesión, el Presidente de aquella, el Diputado Saffirio, exclamó con posterioridad a la misma que: "con las explicaciones dadas, quedamos con la certeza que los controles rigurosos que existen al interior de la PDI permiten que solo puedan operar estos sistemas (Phantom) previa autorización judicial".[46]

Los requisitos de legalidad se cumplirían en tanto se respete la exigencia de la orden judicial previa en caso de medidas vulneratorias de derechos fundamentales, conforme al artículo 9º del Código Procesal Penal. Sin embargo, el uso de malware no está contemplado dentro de

la redacción del código; por tanto, su legalidad estaría condicionada a lo que se busque con su uso, es decir, a que se respeten reglas especiales aplicables, como lo serían las contenidas en las leyes de inteligencia, de conductas terroristas o de drogas, considerando que tales entidades públicas indicaron expresamente que "Phantom" se utilizaría únicamente con miras a perseguir el narcotráfico y crimen organizado en general.[47]

El lenguaje utilizado por la PDI para reconocer el uso de Phantom defiende su uso para la modernización de capacidades de "investigación de crimen organizado, terrorismo internacional y narcotráfico a gran escala".[48] Esas justificaciones utilizan el mismo lenguaje que la Ley 19.974 sobre el sistema de inteligencia del Estado. Dicho cuerpo normativo, en su artículo 24, consagra los "Procedimientos especiales de recolección de información" de fuentes cerradas al público, "limitados exclusivamente a actividades de inteligencia y contrainteligencia que tengan por objetivo resguardar la seguridad nacional y proteger a Chile y su pueblo de las amenazas del terrorismo, el crimen organizado y el narcotráfico", y que incluyen "la intervención de sistemas y redes informáticos" (inciso III, literal b) y "la intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información" (inciso III, literal d). Puesto que tales operaciones se llevan a cabo precisamente por las policías y bajo autorización judicial, esta forma de "intervención" de sistemas informáticos, hecha mediante malware, estaría amparada por la ley.

Sin embargo, difícilmente las disposiciones citadas tuvieron en mente una forma de intrusión tan intensa (y a la vez, riesgosa para la integridad de los sistemas informáticos) como el uso de *malware*. Aun cuando las normas de investigación o de recolección de información con fines de inteligencia puedan entregar un marco legal de operación, estas normas deben ser analizadas en el contexto actual, distinto del de su dictación, y bajo los estándares de debido proceso establecidos en la Constitución y en los tratados internacionales. La sola posibilidad de ser consideradas legítimas no las hace estrictamente necesarias para la investigación, y la sola orden judicial no las hace aceptables, en tanto ponen bajo riesgo seguridad de sistemas y comunicaciones.

Aun si se aceptara su legalidad formal mediante la exigencia de orden judicial, todavía su uso estaría bajo cuestionamiento bajo otros principios de vigilancia estatal. Así, respecto a la proporcionalidad de la medida, analizando esta en relación a una persona que está siendo vigilada a través de "Phantom" hay que evaluar que la herramienta a utilizar sea la menos intrusiva que afecte las libertades fundamentales. En ese sentido, es necesario se demuestre su nececidad teniendo en cuenta la amplia gama de opciones de vigilancia, monitoreo, rastreo, interceptación y registro que existen. Ya el Código Procesal Penal es claro que estas medidas deben ser sumamente acotadas y solo deben permitir el acceso a los datos estrictamente necesarios y nada más. Igualmente, deben ser utilizadas solo en aquellos casos en que no existan otros métodos menos intrusivos y lesivos al derecho a la privacidad.

Desde la mera observación de información públicamente disponible a través de redes sociales, hasta el uso de herramientas de alto nivel de intrusión, el Estado mantiene una gran capacidad de recolección de información e intervención de comunicaciones. Así, sus agentes pueden hacer desde lo más sencillo—identificar a quien convoca a una marcha o manifestación-, pasando por una medida intermedia—solicitar a órganos jurisdiccionales órdenes para obtener información personal e identificar a ciertos usuarios en línea—, hasta la más compleja de todas: usar estas tecnologías para identificar sospechosos y perseguir a estos, única o mayoritariamente, solo tomando en cuenta esta gestión como prueba de su participación criminal.[49] Encontrándose todas estas opciones reñidas con los contenidos propios del derecho a un debido proceso, según el Sistema Interamericano de Derechos Humanos.[50]

2.3 Investigación Sobre Conductas Terroristas

La Ley Nº 18.314 se aplica, en conjunto a la legislación penal de carácter general, en todos aquellos casos en que el delito del que se acusa al investigado reviste el carácter de terrorista según las pautas otorgadas para realizar dicha determinación en el artículo 1º de la misma.

Dado que esta ley permite realizar específicamente interceptación y registro de comunicaciones, sumados a los ya indicados mecanismos probatorios generales del sistema procesal penal y agravados con un mayor tiempo de secreto, esta norma facilita enormemente la labor de vigilancia estatal. Ella otorga facilidades a las facultades intrusivas y dota de mayor opacidad al proceso.

Una crítica usual a esta ley es la definición que entrega sobre actividad terrorista en su primer artículo, dado lo vaga e imprecisa que resulta ésta,[51] al punto que la misma Comisión Interamericana de Derechos Humanos indicó que es tan así que la distinción y calificación de un delito común o un delito terrorista, quedan a la completa discrecionalidad del juez a cargo del caso en concreto.[52]

En efecto, el año 2013 desde el mismo Alto Comisionado de las Naciones Unidas para los Derechos Humanos se hicieron partícipes estas críticas, indicando la falta de un criterio claro y concordante utilizado por los fiscales en Chile al calificar a un delito como terrorista, por ello, sostiene que:

> *"Las diversas justificaciones planteadas han sido subjetivas y carentes de rigor legal. Esto se corrobora al comparar los casos en que se han presentado cargos terroristas y aquellos en que no. Es imposible distinguir una línea divisoria clara y consistente entre casos donde se han presentado cargos como delitos penales comunes (tales como, incendio premeditado, homicidio frustrado y delitos con armas de fuego) de aquellos en que se ha*

> *invocado la ley antiterrorista, a fin de agravar la pena y entregar ventajas procesales adicionales al fiscal. El Relator Especial concluye con reticencia que consideraciones subjetivas, arbitrarias y/o políticas han jugado un papel en la selección de esos casos donde se ha invocado la ley antiterrorista."*[53]

Ahora, que un hecho pase a calificarse como "delito terrorista" importa una serie de medidas de protección adicionales a quienes declaren como testigos en estas causas, mecanismos de delación compensada, aumento de ciertos plazos del proceso penal (como el de detención o de la prisión preventiva), mayor secreto del proceso investigativo y de las pruebas obtenidas en el mismo, y mayores restricciones al ejercicio de algunos derechos constitucionales de los imputados de estas causas.

En relación a la actividad probatoria misma y su nexo con la vigilancia estatal, la ley sobre conductas terroristas permite en su artículo 14 la intercepción, apertura o registro de comunicaciones telefónicas e informáticas y su correspondencia epistolar y telegráfica. Ese permiso se da frente a todas aquellas conductas que califiquen como terroristas por la ley, cuando los hechos se cometan con la finalidad de producir en la población o en una parte de ella el temor justificado de ser víctima de delitos calificados como terroristas. La medida puede otorgarse a petición del Ministerio Público al Juez de Garantía.

A su vez, dada la especial peligrosidad de este tipo de ilícitos, esta ley hace más laxo el estándar exigido para interceptar comunicaciones telefónicas y otro tipo de comunicaciones. Esta ley resta los varios requisitos exigidos en el Código Procesal Penal, reduciéndolos a no interceptar comunicaciones con su abogado y a la necesidad de una resolución fundada emanada del Juez de Garantía en la cual permita la ejecución de éstas.

2.4 Investigación del Tráfico Ilícito de Estupefacientes

La ley 20.000, que sanciona el tráfico ilícito de estupefacientes y sustancias psicotrópicas, establece entre los medios de restricción y otros medios técnicos de investigación la retención o incautación de correspondencia, obtención de copias de comunicaciones o transmisiones, interceptación de comunicaciones. Para ejecutar la medida solo basta la consignación de circunstancias que individualicen al sujeto o lo determinaren, sin necesidad de indicar circunstanciadamente el nombre y dirección del afectado por la medida, según consta en el artículo 24 de esta ley.

La investigación puede ser secreta para los intervinientes cuando lo disponga el Ministerio Público por un plazo máximo de 120 días, renovables sucesivamente por plazos máximos de 60 días; no aplica la posibilidad de control judicial anterior a la formalización establecida en el Código Procesal Penal, mediante la cual cualquier persona que se considerare afectada por una investigación, que no se hubiere formalizado judicialmente, podrá pedir al juez que el fiscal informe sobre los hechos objeto de la investigación o fije un plazo para la misma.

También, sanciona con la pena de presidio menor en su grado medio a máximo a quien informe, difunda o divulgue información relativa a una investigación en curso o amparada por el secreto.

Al igual que la ley 18.314, contempla mecanismos de delación compensada y protección de testigos, también, a partir de su artículo 38 establece medidas en pos de aumentar los plazos y circunstancias del de secreto de la investigación.

Otra semejanza compartida son las críticas a la indeterminación sobre qué constituye un delito propio de esta ley. Al igual que en la "ley antiterrorista", es muy ambigua la calificación penal sobre qué es un delito amparado por esta ley (y con las herramientas de persecución y vigilancia análogas a la ley Nº 18.314) y qué es una conducta impune. Finalmente, ello queda al arbitrio de quien la interpreta y de quien la invoca para investigar y perseguir el delito.

El artículo 24 de esta ley cobra especial relevancia. Esta norma indica que en caso de investigarse delitos propios de esta ley, las medidas de retención, incautación, interceptación de correspondencia como de comunicaciones telefónicas con respecto de cualquier tipo de telecomunicaciones se ven exentas de los requisitos establecidos en el artículo 222 del Código Procesal Penal sobre especificación en la autorización judicial, bastando con solo dar el nombre y dirección del imputado.

Igualmente, esta actividad intrusiva podrá realizarse respecto de toda clase de delitos contenidos en la ley 20.000, como se dijo, sin importar la pena aparejada que tengan. Recordemos que el artículo 222 del Código Procesal Penal, en caso de interceptación de comunicaciones, exige que el delito investigado tenga asociada pena de crimen para la procedencia de la misma.

2.5 Regulación de las Actividades de Vigilancia en el Sistema de Inteligencia Nacional

Con "actividades de inteligencia" nos referimos a todos aquellos medios utilizados para la obtención de información relevante para la seguridad o defensa del Estado, su territorio o la nación que lo habita. Usualmente éstas actividades de inteligencia son mantenidas con carácter secreto o reservado respecto del público en general, con el objeto de resguardar los objetivos de seguridad externa e interna frente al terrorismo internacional y la contingencia nacional e internacional.[54]

En Chile, además, el sistema de inteligencia actualmente vigente se extiende al combate a las actividades de crimen organizado y narcotráfico. Ello amplía la protección del Estado y de la sociedad a otras amenazas internas complejas, aun cuando ellas son comúnmente materia de

competencia de los órganos habituales de investigación y persecución penal.

Según la Constitución, todos los actos, fundamentos y procedimientos de los órganos del Estado son públicos. No obstante, se reserva a una ley de cuórum calificado la determinación de casos en que procede la reserva o secreto, cuando la publicidad afectare el cumplimiento de las funciones de dichos órganos, los derechos de las personas, la seguridad de la Nación o el interés nacional. Es decir, la reserva legal requiere una aprobación parlamentaria alta en la forma, además de objetivos específicos en el fondo, para autorizar que se lleven a cabo actuaciones estatales de forma reservada o secreta.

A ese estándar de aprobación se sujeta cualquier reforma a las actividades de inteligencia autorizadas en reserva, incluyendo aquellas cubiertas por la Ley 19.974 sobre el Sistema de Inteligencia del Estado, de 2004.

2.5.1 Institucionalidad del Sistema de Inteligencia del Estado

Chile establece y regula en el año 2004 el actual Sistema de Inteligencia de Estado, a través de la creación de la Agencia Nacional de Inteligencia (ANI). La ANI distingue, en primer término la inteligencia y la contrainteligencia, considerando la primera como "el proceso sistemático de recolección, evaluación y análisis de información, cuya finalidad es producir conocimiento útil para la toma de decisiones". En segundo término como "aquella parte de la actividad de inteligencia cuya finalidad es detectar, localizar y neutralizar las acciones de inteligencia desarrolladas por otros Estados o por personas, organizaciones o grupos extranjeros, o por sus agentes locales, dirigidas contra la seguridad del Estado y la defensa nacional".

Según la ANI, se conceptualiza como inteligencia el "conocimiento útil, resultado del procesamiento de información, desarrollado por un organismo profesional, para asesorar en sus decisiones a los niveles superiores del Estado, con el objetivo de prevenir e informar los riesgos a los intereses nacionales y el logro de los objetivos del país, la seguridad y la defensa".

La ANI encabeza los servicios de inteligencia en Chile. El sistema de inteligencia está formado también por los servicios de inteligencia de las distintas ramas de las Fuerzas Armadas y de Orden, incluyendo a la Dirección de Inteligencia de Defensa del Estado Mayor de la Defensa Nacional las Direcciones de Inteligencia de cada una de las Fuerzas Armadas y las Direcciones o Jefaturas de Inteligencia de las Fuerzas de Orden y Seguridad Pública.

Esta Agencia Nacional de Inteligencia realiza funciones de recolección y procesamiento de información a nivel nacional e internacional; elabora informes periódicos, de carácter secreto, para ser presentados al Presidente de la República; propone normas y procedimientos de protección de los sistemas de información; hace requerimientos de

información a los organismos de inteligencia de las Fuerzas Armadas y de las Fuerzas de Orden y Seguridad pública, entre otros; dispone la aplicación de medidas de inteligencia con objeto de detectar, neutralizar y contrarrestar las acciones de grupos terroristas, nacionales o internacionales, y de organizaciones criminales transnacionales; y dispone actividades de contrainteligencia.

En rigor, la ANI carece de capacidad operativa para actividades de intervención con fines de inteligencia: si bien puede recolectar y procesar información, las vías para su obtención están reservadas a los órganos de inteligencia ya referidos. Así, la ANI mantiene, como órgano, una capacidad más bien estratégica y política.

2.5.2 Recolección de Información y Actividades de Inteligencia

La primera forma de recolección contempla la actuación dentro de las facultades legales del artículo 8º de la Ley, entre las que se cuentan, de forma general, la recolección otros y procesamiento de información, informes, propuestas, y requerimientos de información a otros órganos. Es decir, es útil recolectar y procesar tanto lo informado por los órganos requeridos, como lo obtenido de actividades diarias tales como el análisis de fuentes abiertas de información, como la prensa.

Dentro de los órganos a los cuales se puede requerir información se encuentran tanto a los organismos de Inteligencia de las Fuerzas Armadas como de las Fuerzas de Orden y Seguridad Pública (las policías: Carabineros de Chile, y la Policía de Investigaciones de Chile) como de Gendarmería. Igualmente, pueden requerir la información que estimen necesaria para el cumplimiento de sus objetivos a los diversos órganos pertenecientes a la Administración del Estado y a empresas e instituciones que cuenten con aporte estatal.

Una segunda forma de proceder supone la imposibilidad de obtener la información por medio de fuentes abiertas, tanto que están públicamente disponibles como la que puede obtenerse previo requerimiento de información a un órgano estatal, siendo esta estrictamente indispensable para el cumplimiento de la seguridad nacional y la protección de Chile y su pueblo de las amenazas del terrorismo, el crimen organizado y el narcotráfico. Se autorizan los “procedimientos especiales de obtención de información”, que permiten el acceso a antecedentes relevantes contenidos en fuentes cerradas o que provienen de ellas, y que aporten antecedentes necesarios al cumplimiento de la misión específica de cada organismo operativo (Artículo 24).

Estas medidas contemplan procedimientos de intervención telefónica, informática y radial; intervención de sistemas y redes informáticas; escuchas y grabaciones electrónicas; intervención de cualquier otro sistema tecnológico destinado a la transmisión, almacenamiento o procesamiento de las comunicaciones electrónicas.
Respecto a los criterios de uso de estos procedimientos especiales de obtención de

información, la ley indica que se usarán en caso que sean estrictamente indispensables para el cumplimiento de los objetivos del Sistema (Principio de Necesidad). Además, se delimita su utilización a actividades de inteligencia y contrainteligencia que tengan por objetivo resguardar la seguridad nacional y proteger a Chile y su pueblo de las amenazas del terrorismo, crimen organizado y narcotráfico (Principio de Proporcionalidad) en sentido estricto), según contempla el artículo 23 de esta ley. El requisito de idoneidad propio de la aplicación de un test de proporcionalidad lo podemos encontrar en que no existe una fuente pública (en los términos ya expuestos) menos lesiva que permita obtener estos datos.

Para la concreción de procedimientos especiales contemplados en la ley es requerida autorización judicial, que debe ser solicitada por los directores o jefes de los organismos de inteligencia, con el único objetivo de resguardar la seguridad nacional y proteger a Chile y a su pueblo de las amenazas del terrorismo, crimen organizado y narcotráfico.

La autorización la emite directamente el Ministro de Corte de Apelaciones del territorio donde se realiza la diligencia o donde se inicia la misma, o a través del juez institucional que corresponda. Así, la autorización no será vista por un Juez de Garantía como en el sistema común de recolección de información, sino por un ministro de corte o bien por un juez castrense. Excepcionalmente, la ley autoriza al uso de agentes secretos con la facultad de infiltrarse (artículo 31) y de informantes (artículo 32), sin necesidad de autorización judicial.

2.5.3 Usos Posibles de la Información Obtenida por la ANI por Otros Organismos del Estado

El artículo 42 de la ley establece que la información que recopilen, elaboren o intercambien los organismos que conformen el Sistema deberá utilizarse exclusivamente para el cumplimiento de sus respectivos cometidos.

En tal sentido, el objetivo central de los organismos de inteligencia es la asesoría al Presidente de la República, a quien, en cumplimiento de las labores de inteligencia, efectuarán apreciaciones globales y sectoriales, realizarán informes periódicos, propondrán normas y procedimientos de protección, y dispondrán la aplicación de medidas de inteligencia contrainteligencia, entre otras funciones señaladas en el artículo 8.

Por regla general, los organismos del Estado no tienen acceso a la información obtenida por la ANI, al presentar carácter secreto y de circulación restringida. Excepcionalmente podrán entregarse datos solicitados por la Cámara de Diputados, el Senado, los Tribunales de Justicia, el Ministerio Público, la Contraloría General de la República por intermedio de los Ministros de Interior, de Defensa Nacional y el Director de la Agencia, sin perjuicio que las autoridades y los funcionarios que hubieran tomado conocimiento de los antecedentes a que se refiere el inciso anterior estarán obligados a mantener el carácter secreto de su existencia y contenido aún después del término de sus funciones en los respectivos servicios.

2.5.4 Casos

No existe información pública sobre la actividad de los organismos de inteligencia, ni de las medidas intrusivas que adoptan con fundamento en la seguridad nacional, defensa y cumplimiento de objetivos estatales. Solamente es conocida su acción en determinados hechos y conflictos.

Por ejemplo, la investigación por uso de artefactos explosivos conocida como el "caso Bombas",[55] y la participación en un conflicto en el sur de Chile en relación con hechos de violencia vinculados con demandas del pueblo mapuche, que diversos órganos del Estado han calificado como terroristas. Sobre esto último, la Comisión de Defensa del Senado convocó a sesión (secreta) al director de la ANI a principios de 2013, sin mayor información sobre sus procedimientos en la zona.[56]

Respecto del caso Bombas, no se logró la condena a título de delitos terroristas pese a esfuerzos del Ministerio Público, la Policía de Investigaciones y la ANI. No obstante, se acusó por medios de prensa a los órganos de persecución por llevar una investigación poco transparente y lesiva de garantías constitucionales, incluyendo la realización de escuchas telefónicas e interceptación de correos electrónicos sin autorización judicial previa. El director de la ANI fue citado más de una vez ante la comisión respectiva de la Cámara de Diputados para dar cuenta de tales hechos, en sesión secreta.

No obstante, puesto que no existe información pública sobre la actividad de la ANI, las actividades de inteligencia que han sido conocidas como vulneratorias de la privacidad han sido fundamentalmente de gobiernos extranjeros, por medio de filtraciones de información a la prensa o bien por información pública no detallada. Tanto las actividades de control de legalidad por parte de las Cortes de Apelaciones como el control político por parte del Congreso Nacional, se encuentran fuera del escrutinio público.

3.
Análisis de la Normativa Chilena a la Luz de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de la Comunicaciones

En este apartado tratarán cada uno de los principios ya indicados en el título y veremos qué tanto apego a estos tiene la normativa nacional que permite la actividad de vigilancia estatal.[57]

Legalidad

> *Cualquier limitación a los derechos humanos debe ser prescrita por ley. El Estado no debe adoptar o implementar una medida que interfiera con los derechos a la privacidad en ausencia de una ley públicamente disponisble, que cumpla con estándar de claridad y precisión suficientes para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación.*

Este principio importa que toda limitación a los derechos humanos debe estar prescrita por ley, a contrario sensu, no es legítima una actividad vulneratoria de estos que no esté autorizada legalmente.

Según se indicó, todo el sistema procesal penal, desde lo más general (Código Procesal Penal) hasta lo más específico (leyes de persecución de delitos en particular), es informado por el principio general contemplado en el artículo 9 del Código Procesal Penal: Toda actuación del procedimiento que vulnere los derechos fundamentales del investigado o terceros debe contar con una autorización judicial previa. Luego, cada una de las medidas intrusivas tratadas en específico contemplan la necesidad de tal autorización, además de otros requisitos legales.

Por tanto, este principio se cumpliría en la legislación chilena procesal, mas debe ponerse atención en la indeterminación típica ya señalada que existe a la hora de calificar algunos delitos asociados a las leyes Nº 20.000 y Nº 18.314. Así, es perentorio aclarar los casos en que puede procesarse por alguna de estas leyes de forma tajante, tal y como ya han observado organizaciones internacionales al respecto. Igualmente, existen problemas con iniciativas como el uso de "Phantom", según ya analizamos.

En relación a la Ley de Protección de Datos Personales, esta permite que los organismos públicos puedan tratar aquellos sin autorización de su titular, siempre y cuando sea en el marco de sus funciones. Lo anterior, si bien es una de las excepciones legales a la normativa protectora, a su vez crea un espacio indeterminado para el tratamiento de datos personales realizado en secreto, el cual podría realizarse en base a datos obtenidos a través de actividades de vigilancia estatal.

Objetivo Legítimo

> *Las leyes sólo deberían permitir la Vigilancia de las Comunicaciones por parte de autoridades estatales específicas para alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante e importante y que sea necesario en una sociedad democrática. Cualquier medida no debe aplicarse de manera que discrimine con base en raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición.*

La idea general es que en el sistema jurídico chileno la actividad de vigilancia efectuada por entes públicos está dirigida a la persecución criminal. Como podemos ver tanto en el Código Procesal Penal y en las leyes sobre delitos específicos, para poder recurrir a estas medidas intrusivas se requieren de ciertos pisos mínimos, ya sea que una conducta esté tipificada como un delito de especial peligrosidad, como lo son los actos terroristas o el tráfico de sustancias psicotrópicas, o que un delito genérico presente una pena de crimen (que inician en cinco años y un día).

Es decir, los resguardos legales apuntan a que, medidas tan lesivas como la interceptación de telecomunicaciones, apunten a la obtención de información allí donde se busque la persecución de delitos particularmente graves, y en la medida en que se enfoque en las personas relacionadas con los mismos.

Si bien esto es cierto respecto de la interceptación de telecomunicaciones, no parece igualmente cierto respecto de otras medidas, como la retención e incautación de correspondencia, cuya regulación es la utilizada en la práctica para requerir la incautación física de equipos que alojan copias de correos electrónicos.

Según el Artículo 218 del Código Procesal Penal, previa solicitud del Ministerio Público, el juez puede ordenar la retención de la correspondencia postal, telegráfica o de otra clase y los envíos dirigidos al imputado o remitidos por él o de los que pudiere ser el destinatario, cuando por motivos fundados fuere previsible su utilidad para la investigación. En casos como este, es solamente la posible utilidad para la investigación, independientemente de que

se investigue un delito menos grave, lo que hará procedente tal medida.

Necesidad, Idoneidad y Proporcionalidad

> *Necesidad: Leyes de vigilancia, reglamentos, actividades, poderes o autoridades deben limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo. La Vigilancia de las Comunicaciones sólo debe llevarse a cabo cuando es el único medio para alcanzar un objetivo legítimo, o bien cuando habiendo varios medios sea el menos propenso a vulnerar los derechos humanos. La carga de establecer esta justificación, tanto en los procesos judiciales como en los legislativos, recae en el Estado.*
>
> *Idoneidad: Cualquier caso de Vigilancia de las Comunicaciones autorizado mediante ley debe ser apropiado para cumplir el objetivo legítimo específico identificado.*
>
> *Proporcionalidad: La Vigilancia de las Comunicaciones debería ser considerada como un acto altamente intrusivo que interfiere con los derechos humanos, amenazando los cimientos de una sociedad democrática. Las decisiones sobre la Vigilancia de las Comunicaciones deben considerar la sensibilidad de la información accesible y la gravedad de la infracción sobre los derechos humanos y otros intereses en competencia.*

Estos Principios se tratarán en conjunto como parte del test de proporcionalidad, reconocido por la doctrina y la jurisprudencia, y que debe llevar a cabo un juez previo a autorizar la ejecución de actividad probatoria vulneratoria de derechos fundamentales, test que igualmente debe aplicar un juez en caso de encontrarse en una colisión de este tipo de derechos.

La legislación aplicable no hace mención específica a estos principios, pero ello se subentiende. Así, por ejemplo, en relación al señalado artículo 222 del Código Procesal Penal, los límites temporales de la medida intrusiva, que se acote su margen a solo los datos estrictamente necesarios o a los soportes que los contienen, que se acredite un cierto nivel de probabilidad ("fundada sospecha") de que el investigado pudo estar involucrado en el delito cometido, y la exigencia de una pena mínima o una calificación especial atribuible a la conducta criminal desplegada, delimitan la procedencia de tales medidas, acotando lo que puede ser interceptado y registrado.

Sumando a lo anterior, en el caso de la interceptación de telecomunicaciones, existe un mandato a las empresas de servicios de telecomunicaciones de no divulgación de dichas

comunicaciones y otro dirigido a tomar resguardos al realizar estas prácticas intrusivas. Finalmente, se llama a borrar los contenidos obtenidos con la actividad vulneratoria que excedan a lo judicialmente permitido y pasado un determinado plazo, se debe borrar todo lo obtenido de esta forma.

El Principio de Necesidad se ve implícitamente recogido al enunciarse que el juez de garantía autorizará tales diligencias en caso de que la investigación del hecho lo hiciere imprescindible. Nuevamente, en la normativa sobre interceptación de comunicaciones es posible ver cada uno de ellos contemplados y efectivamente aplicados por la intervención del juez de garantía.

Se debe tomar en cuenta nuevamente el caso "Phantom", considerando que dicho software permite interceptar estas de forma remota y silenciosa. De utilizarse este sistema para dicha función, sin cumplir con el marco exigido por los artículos 222 y siguientes y sin orden judicial expresa, habría una clara infracción a estos tres principios.

Como segundo contraste, la ya mencionada incautación de correspondencia, al aplicarse concretamente a propósito de correos electrónicos, no cumple con el mismo test de proporcionalidad, ni aparece como ajustada a un estándar constitucional de protección de derechos fundamentales.

Aun aceptando la posible idoneidad de la incautación de equipos informáticos o computacionales que alojen correos electrónicos, su procedencia como medida para la investigación criminal, según el mismo lenguaje legal, no requiere necesidad, sino mera conveniencia para los fines de la investigación. Asimismo, constituye un nivel excesivo de afectación de la privacidad de la persona en cuestión el retiro de equipos computacionales con la totalidad de sus correos electrónicos con igual nivel de accesibilidad, frente a aquello que efectivamente sería útil para una investigación.

Autoridad Judicial Competente

> *Las decisiones relacionadas con la Vigilancia de las Comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente.*

Además de los requisitos mencionados a propósito de cada medida intrusiva, incluida la interceptación de telecomunicaciones, reiteramos el artículo 9 del Código Procesal Penal, norma que actúa como principio formativo de la legislación procesal penal en su totalidad, disposición que recalca la necesidad de una autorización judicial previa en caso de actuaciones dentro del procedimiento criminal que puedan afectar o vulnerar los derechos fundamentales del investigado o de terceros. Esta es la regla general.

No obstante, la práctica relativa a la entrega de datos de comunicación, muestra que en ocasiones las policías han solicitado tales datos por parte de quienes los mantienen, buscando una colaboración con la investigación que haga innecesaria la orden judicial.[58]

Debido Proceso

> *El debido proceso exige que los Estados respeten y garanticen los derechos humanos de las personas asegurando que los procedimientos legales que rigen cualquier interferencia con los derechos humanos estén enumerados apropiadamente en la ley, sean practicados consistentemente y estén disponibles para el público general.*
>
> *Específicamente, al decidir sobre sus derechos, toda persona tiene derecho a una audiencia pública y justa dentro de un plazo razonable por un tribunal independiente, competente e imparcial establecido por ley, salvo en casos de emergencia donde exista un riesgo inminente de peligro para la vida humana. En tales casos, debe buscarse una autorización con efecto retroactivo dentro de un plazo razonable y factible. El mero riesgo de fuga o de destrucción de pruebas no se considerará suficiente para justificar la autorización con efecto retroactivo.*

Principio ampliamente contenido en la legislación chilena, tanto en la Constitución como en los Tratados Internacionales de Derechos Humanos que son aplicables como parte del bloque de constitucionalidad, como dentro de la misma legislación procesal penal.

En efecto, la regulación constitucional de este derecho, si bien no usa este término exactamente (pues habla del derecho a un procedimiento e investigación racionales y justos), su contenido esencial es similar a lo recogido en el artículo 8.1 de la Convención Americana sobre Derechos Humanos.

Igualmente, los diez primeros artículos del Código Procesal Penal, contenidos en el primer título de esta norma llamado "Principios Básicos", contempla una serie de garantías relacionadas a este derecho humano, tales como: Juicio único y natural, exclusividad y unicidad de la investigación penal, presunción de inocencia, legalidad de las medidas restrictivas o privativas de libertad, protección a la víctima, ámbito de la defensa, garantías y reconocimientos al imputado, contemplación de una audiencia de control de garantías y la necesidad de la orden judicial previa que autorice gestiones investigativas vulneratorias de derechos fundamentales.

De manera más relevante, las reglas del Código Procesal Penal permiten la exclusión de la

prueba ilícita, esto es, de las obtenidas con incumplimiento de las normas legales, incluyendo el resguardo general de respeto a los derechos fundamentales y orden judicial previa.

Notificación del Usuario

> *Aquellos cuyas comunicaciones están siendo vigiladas deben ser notificados de la decisión de autorizar la Vigilancia de Comunicaciones con el tiempo y la información suficiente para que puedan impugnar la decisión o buscar otras soluciones y deben tener acceso a los materiales presentados en apoyo de la solicitud de autorización. El retraso en la notificación solo se justifica en las siguientes circunstancias:*
>
> *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; y 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; y el usuario afectado se notifica tan pronto como el riesgo desaparece según lo determinado por la autoridad judicial competente.*
>
> *La obligación de notificar recae en el Estado, pero los proveedores de servicios de comunicaciones debe tener la libertad de notificar a las personas de la Vigilancia de las Comunicaciones, de forma voluntaria o bajo petición.*

En relación a la interceptación de comunicaciones, el artículo 224 del Código Procesal Penal es claro: "La medida de interceptación será notificada al afectado por la misma con posterioridad a su realización, en cuanto el objeto de la investigación lo permitiere, y en la medida que ello no pusiere en peligro la vida o la integridad corporal de terceras personas".

Luego, dicha disposición redirige al artículo 182 de ese mismo cuerpo normativo, norma en la cual se decreta que las actuaciones investigativas de la Fiscalía son secretas para terceros ajenos al proceso, mas el secreto deja de ser la norma general en caso de los intervinientes del mismo, salvo ciertas excepciones en que se permite aquél, las cuales, como sea, tienen un límite de 40 días de duración.

Transparencia

> *Los Estados deben ser transparentes sobre el uso y alcance de las leyes de Vigilancia de las Comunicaciones, reglamentos, actividades, poderes o autoridades. Deben publicar, como mínimo, información global*

sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora, el tipo y propósito, y el número específico de personas afectadas por cada una y según el tipo de investigación y sus propósitos.

Los Estados deben proporcionar a las personas la información suficiente para que puedan comprender plenamente el alcance, naturaleza y aplicación de las leyes que permiten la Vigilancia de las Comunicaciones.

Los Estados no deberían interferir con los proveedores de servicios en sus esfuerzos para publicar los procedimientos que aplican en la evaluación y el cumplimiento de solicitudes de los Estados para la Vigilancia de Comunicaciones, se adhieran a esos procedimientos, y publicar los registros de las solicitudes de los Estados para la Vigilancia de las Comunicaciones.

En el informe anual elaborado por el Ministerio Público no se da cuenta de la cifra de utilización de este tipo de medidas. De la misma forma, no existe norma alguna que permita a las personas directamente afectadas por estas medidas conocer de la existencia de las mismas, ni recibir comunicación de que se han entregado sus datos.

Cualquier reporte sobre las medidas podría, en teoría, solicitarse de forma posterior y mediante mecanismos de transparencia pasiva. Esta característica es transversal al sistema de persecución penal en Chile, donde la adopción de medidas intrusivas sobre comunicaciones llega a ser conocida allí donde se utiliza efectivamente como prueba en el proceso penal.

Plataformas como Facebook y Twitter realizan su informe de transparencia anual[59] en los cuales es posible conocer el número de solicitudes de información de diversos Gobiernos, estando el chileno entre aquellos.

Supervisión Pública

Los estados deberían establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la Vigilancia de las Comunicaciones.

En Chile no se cuenta con un organismo independiente que revise este tipo de prácticas. Lo más cercano podrían ser los tribunales superiores de justicia a través de los recursos establecidos en el Código Procesal Penal y el Tribunal Constitucional en caso de conocer una acción constitucional referida a casos de abuso de medidas vulneratorias de derechos

fundamentales.

Igualmente, los Jueces de Garantía tienen instancias para revisar lo anterior, tanto como la cautela de garantías como las causales de exclusión de prueba, donde se contempla la prohibición del uso de prueba ilícita. Fuera de ello, el sistema procesal penal chileno carece de un mecanismo independiente de supervisión para garantizar la transparencia y la rendición de cuentas de la vigilancia de las comunicaciones.

Ligeramente distinto es el caso de las actividades de vigilancia, donde además del control judicial de las medidas, existe la posibilidad de control democrático por parte del Congreso. No obstante, las instancias son de carácter informativo, con control de corte político, y sin resultados públicamente verificables por tratarse de comisiones reservadas.

Integridad de las Comunicaciones y Sistemas

> *A fin de garantizar la integridad, seguridad y privacidad de los sistemas de comunicaciones, y en reconocimiento del hecho de que poner en peligro la seguridad con fines estatales casi siempre afecta la seguridad en términos generales, los Estados no deben obligar a los proveedores de servicios o proveedores de "hardware" o "software" a desarrollar la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de Vigilancia de las Comunicaciones del Estado.*
>
> *La retención o la recopilación de datos a priori nunca debe ser exigida a los proveedores de servicios. Las personas tienen el derecho a expresarse anonimamente, por lo que los Estados deben abstenerse de obligar a la identificación de los usuarios.*

La legislación procesal penal nacional obliga a los ISP a, por lo menos durante un año, llevar registro del rango de números IP y de las conexiones que hagan sus abonados, lo anterior con tal de facilitar la puesta en práctica de la medida intrusiva de interceptación de comunicaciones establecida en el artículo 222 del Código Procesal Penal.

Como ya se dijo, es posible encontrar en mayor profundidad cómo se realiza esto en el reglamento correspondiente. Si bien no existen obligaciones de instaurar mecanismos de vigilancia dentro de las características técnicas físicas o lógicas de los sistemas de comunicación, esta retención de datos obligatoria va en abierta contraposición al principio.

Garantías para la Cooperación Internacional

> *En respuesta a los cambios en los flujos de información y en las*

tecnologías y servicios de comunicaciones, los Estados pueden necesitar procurar la asistencia de un proveedor de servicios extranjero y otros Estados. En consecuencia, los tratados de asistencia judicial recíproca (MLAT, por sus siglas en inglés) y otros acuerdos celebrados por los Estados deben garantizar que, cuando la legislación de más de un Estado pueda aplicarse a la Vigilancia de las Comunicaciones, se adopte el estándar disponible con el mayor nivel de protección para las personas.

El principio de la doble incriminación debe ser aplicado en el momento en que los Estados procuren asistencia para efectos de hacer cumplir su legislación interna. Los Estados no pueden utilizar los procesos de asistencia judicial recíproca y las solicitudes extranjeras de Información Protegida para burlar las restricciones del derecho interno relativas a la Vigilancia de las Comunicaciones.

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

La Convención Interamericana sobre Asistencia Mutua en Materia Penal (MLAT, por sus siglas en inglés)[60], al referirse a la aplicación y alcance de la convención en su segundo artículo indica que se aplica únicamente a la prestación de asistencia mutua entre los Estados Partes, así, sus disposiciones no otorgan derecho a los particulares para obtener o excluir pruebas, o para impedir la ejecución de cualquier solicitud de asistencia.

Esta es la única disposición de este tratado aplicable a materia de vigilancia, ello por tanto si una legislación contempla una protección menor a la privacidad de sus habitantes, no se puede utilizar este instrumento internacional para eludir un régimen más garantista.

A su vez, igualmente puede utilizarse en sentido inverso: un Estado Parte con una legislación con mayores estándares de protección de derechos fundamentales tampoco podría excusarse ante una petición proveniente de otro donde el marco sea más permisivo. Lo anterior, sin perjuicio de lo dispuesto en la Convención Interamericana sobre Derechos Humanos referentes al respeto y adecuación de la legislación interna de tales derechos.

Es en base a este tratado que existió intercambio de información en un caso llamado "Los Luksic", en que el titular de una cuenta de parodia de Twitter, en Chile, fue perseguido por el delito de usurpación de nombre. Siguiendo las vías diplomáticas propias del tratado, se solicitó información a Twitter en los Estados Unidos, que entregó la información disponible bajo el entendido de que se trataba de una "usurpación de identidad", como delito afín en ese país.[61] No obstante, ambos delitos no son equiparables en los elementos del tipo penal.

La cooperación en la entrega de datos fue, en este caso, más allá de cualquier garantía sobre los derechos de la persona afectada, incluyendo la necesidad de doble incriminación. El caso fue finalmente desestimado por falta de acreditación de la concurrencia del delito.[62]

Además del MLAT regional, existe desde su firma en 2014, el Convenio de cooperación en la prevención y combate del delito entre Chile y Estados Unidos[63], tratado bilateral que no contempla una disposición que indique que debe aplicarse la legislación del Estado Parte que respete de mayor forma la privacidad del afectado.

Pese a dicha ausencia, sí considera otra serie de resguardos a los derechos fundamentales del individuo, dentro de los cuales tenemos: no comunicación de datos hasta que el Estado receptor haya adoptado todas las medidas de resguardo adecuadas, que la parte que envía los datos no puede establecer como condición para dicho envío que el Estado receptor modifique sus criterios legales para procesar datos personales (dentro de lo que cabría que no se puede usar este tratado para eludir la legislación interna), se contempla el principio de transparencia en la entrega de información a los titulares de datos y se hace mención expresa a mecanismos de corrección, bloqueo y eliminación de datos.

Garantías contra el Acceso Ilegítimo y Derecho a Recurso Efectivo

> *Los Estados deben promulgar leyes que penalicen la Vigilancia de las Comunicaciones ilegal por parte de actores públicos o privados. La ley debe proveer sanciones penales y civiles suficientes y adecuadas, protección a los "whistleblowers" y medios de reparación a las personas afectadas. Las leyes deben estipular que cualquier información obtenida de una manera que sea inconsistente con estos principios es inadmisible como prueba en cualquier procedimiento, al igual que cualquier prueba derivada de dicha información.*
>
> *Los Estados también deben promulgar leyes que establezcan que, después de que el material obtenido a través de la Vigilancia de las Comunicaciones ha sido utilizado con la finalidad por el que fue obtenida la información, el material no debe ser retenido, en su lugar, debe ser destruido o devuelto a los afectados.*

Si bien la Ley de Delitos Informáticos chilena ha sido ampliamente criticada por su brevedad y lo anticuado de su contenido, incluso aquella contempla una figura penal asociada a los accesos ilegítimos a sistemas de información en el artículo 2 de la Ley Nº 19.223 que tipifica figuras penales relativas a la informática, el cual contempla que "El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".

Como se puede señalar, aquí se contempla, con ciertas falencias[64], la figura del espionaje informático, pero dicha ley carece de una tipificación del delito de interceptación de comunicaciones no autorizadas. Solo establece que las empresas a cargo de cumplir con esta medida no podrán dar a conocer el contenido de las comunicaciones interceptadas, salvo que sean citados a declarar en el marco del proceso penal. Es de gravedad que, en caso de infracción a lo anterior, no se establezca una sanción específica.

El Código Penal, en su artículo 161-A, contempla una figura genérica sobre quien capte, grabe, intercepte o reproduzca conversaciones privadas sin autorización. La pena asociada solo es de reclusión menor o multa, la que se aplica aumentada a quien divulgue las conversaciones que él o ella misma obtuvo.

En relación a esto último, encontramos la regulación sobre la prueba en el sistema procesal penal tanto respecto de la prohibición de la prueba obtenida con vulneración de derechos fundamentales (prueba ilícita) como la prohibición de utilización como medio de prueba de los resultados obtenidos de una interceptación telefónica u otra medida intrusiva en caso que ella no cumpla con los requisitos legales.

Además, esta normativa contempla que pasado el lapso otorgado para realizar la interceptación, esta deberá finalizarse y se deben borrar los datos obtenidos a través de dicha medida. Igualmente, deben borrarse todas aquellos antecedentes que excedan del contenido de la autorización de la medida, límites que constan en la autorización judicial previa.

4.
Recomendaciones

En base a la labor comparativa realizada en el capítulo anterior, se propondrán una serie de recomendaciones al Estado chileno en torno al debido resguardo de los Derechos Humanos de los individuos ante la actividad de vigilancia realizada por el aparato público.

- Establecer tipos penales que permitan definir claramente cuándo se está ante un delito procesable por leyes penales especiales, considerando que estos cuerpos normativos rebajan los estándares de exigencia a la hora de autorizar labores de investigación criminal invasivas.
- Extender los requisitos de procedencia exigidos a la medida intrusiva de interceptación telefónica y de otro tipo de telecomunicaciones a la totalidad de estas. La diferencia entre los altos estándares exigidos para solo una de aquellas carece de sustento alguno.
- Aplicar pisos mínimos de penas asociadas al hecho investigado para poder acceder a medidas intrusivas y de vigilancia de mayor intensidad. Que la peligrosidad misma del delito se condiga con las medidas intrusivas asociadas a su investigación.
- Establecer sanciones específicas y de mayor intensidad a las empresas de telecomunicaciones encargadas de realizar labores de interceptación y registro, cuando les sea solicitado, en caso de divulgación, conservación o uso indebido de los datos así conseguidos.
- A su vez, modificar la anticuada Ley de Delitos Informáticos por una que tipifique y castigue las conductas de vigilancia ilegítimas.
- Mayor rigurosidad judicial y policial tanto al autorizar el ejercicio de medidas de vigilancia como a la hora de ponerlas en práctica.
- Ser estrictos en la observancia de los requisitos de procedencia de las medidas de vigilancia, sobre todo, en la necesidad de autorización judicial previa.
- Transparencia activa por parte del Ministerio Público en lo referente a cifras de solicitudes enviadas al tribunal y las medidas intrusivas efectivamente ejecutadas.
- En los próximos acuerdos de cooperación internacional referidos a combate del crimen incluir disposiciones que hagan aplicable la legislación que garantice de mejor forma los derechos humanos del afectado.
- Reducir al mínimo la actividad de vigilancia. Que su procedencia solo recaiga en comisión de delitos de alta peligrosidad; con un marco, tanto de contenido como temporal, previamente delimitado por un juez, que tal medida esté consagrada en la ley con causales específicas que permitan su puesta en práctica y, en caso alguno, utilizarlas para perseguir a disidentes ideológicos o para vigilar masivamente a la población.[65]

5.
Conclusiones

Como se aprecia, no existe un solo cuerpo legislativo en el cual se contenga toda la base legal que permite la actividad de vigilancia estatal, a su vez, las garantías de los habitantes chilenos ante tal intrusión, principalmente, a sus derechos a la privacidad y libertad de expresión se encuentran también dispersas, entre Constitución, leyes e, incluso, Tratados Internacionales.

La jurisprudencia constitucional no se ha referido en relación a la vulneración de estos derechos como consecuencia de actos de vigilancia del poder público, mas podemos recurrir a la jurisprudencia interamericana donde sí existen tales pronunciamientos y a las sentencias sobre aquellos derechos en el ámbito nacional y aplicar los estándares allí definidos a estos casos.

En Chile, el marco legal que sustenta la vigilancia estatal lo podemos encontrar en el ámbito de la persecución penal, especialmente, en el Código Procesal Penal como norma guía y luego en una serie de legislaciones sobre delitos o servicios en particular, las cuales siguen la base del código, añadiendo modificaciones a la procedencia de esta actividad intrusiva, usualmente siento más permisivos en el ejercicio de estas, considerando la peligrosidad de los delitos que tratan, además de verse agravado por calificaciones penales amplias y vagas.

Se toma como base la medida de interceptación telefónica y de otro tipo de telecomunicaciones por ser la más extensamente tratada así como también una de las más aplicadas. Es necesario insistir en que si bien aquella cuenta con una regulación bastante estricta y garantista, en la práctica su aplicación (y la de otras medidas de similar envergadura) no siempre resultan tan protectoras de los derechos humanos de los investigados, como también existe una discriminación arbitraria en la cual a la interceptación telefónica se le exigen mayores estándares y a las demás medidas intrusivas no, siendo que todas ellas son igualmente invasivas.

Por ejemplo, hoy un teléfono celular no solo sirve para llamar. Así sería más simple pedir como incautación de objeto el móvil del imputado que solicitar la interceptación de las llamadas realizadas con el mismo, pues no solo es una medida más simple de autorizar, sino que también que con ello se puede acceder a correos electrónicos, redes sociales, aplicaciones de mensajería, registros de llamadas, historiales de navegación, entre otros.

Es posible notar que, salvo los problemas anteriormente indicados, la legislación chilena cumple mayoritariamente con los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.

No obstante, se debe poner atención en actuaciones de vigilancia estatal que no se encuentra específicamente autorizadas por la ley, como la más reciente compra del sistema "Phantom" por parte de la Policía de Investigaciones a Hacking Team y las implicancias que ello puede tener, respecto a la vulneración de estos principios.

1 United Nations, "The right to privacy in the digital age Report of the Office of the United Nations High Commissioner for Human Right", 2014. pp. 3-4. https://eff.org/r.hz9z [Fecha de consulta: 24 de Julio, 2015].

2 En Chile, la ley permite (Ley N° 19.974) que cuando determinada información sea "estrictamente indispensable para el cumplimiento de los objetivos del Sistema de Inteligencia del Estado y no pueda ser obtenida de fuentes abiertas" (artículo 23), se utilicen procedimientos especiales de obtención de información que se listan. Dichos procedimientos están limitados "a actividades de inteligencia y contrainteligencia que tengan por objetivo resguardar la seguridad nacional y proteger a Chile y su pueblo de las amenazas del terrorismo, el crimen organizado y el narcotráfico" (artículo 23). Tales procedimientos incluyen "a) La intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas; b) La intervención de sistemas y redes informáticos; c) La escucha y grabación electrónica, incluyendo la audiovisual, y d) La intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información" (artículo 24).

3 Derechos Digitales, "Policía de Investigaciones de nuevo vulnera privacidad en Internet", Derechosdigitales.org. 15 de octubre de 2010. https://eff.org/r.rf9p [Fecha de consulta: 03 de Junio, 2015].

4 Francisca Rivas, "En libertad queda joven acusado de agredir a carabinero: pruebas sólo eran fotos de Facebook", Rabio Bío Bío, 20 de mayo de 2014. https://eff.org/r.4u9z [Fecha de consulta: 03 de junio, 2015].

5 Andrés López, "Aumentan solicitudes de antecedentes a Twitter por amenazas", La Tercera. 16 de febrero de 2013. https://eff.org/r.6nuh [Fecha de consulta: 03 de Junio, 2015].

6 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/text; EFF, ARTICLE19, Análisis Jurídico Internacional de Apoyo y Antecendentes de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/AnalisisLegal; Access, Guía Universal de Implementación de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://eff.org/r.4gac [Fecha de consulta: 20 de Julio, 2015].

7 Ibid.

8 La Carta Fundamental chilena, al tratar la soberanía, en el artículo 5º, inciso segundo, expresa: "El ejercicio de la soberanía reconoce como limitación el respeto a los derechos esenciales que emanan de la naturaleza humana. Es deber de los órganos del Estado respetar y promover tales derechos, garantizados por esta Constitución, así como por los tratados internacionales ratificados por Chile y que se encuentren vigentes". Como consecuencia de esta disposición es que se habla que en Chile, además de la legislación interna sobre este tipo de derechos (la misma Constitución), se debe considerar el llamado bloque de constitucionalidad.

9 Se ha discutido el rango de los derechos consagrados en tratados internacionales sobre derechos humanos dentro del ordenamiento jurídico chileno, esto es, si son de jerarquía constitucional o meramente legal. La jurisprudencia de la última década ha definido que tienen un rango supralegal y, al menos, equivalente al constitucional.

10 Nos basamos parcialmente en lo ya expuesto en Lara, J., C. Pincheira, y F. Vera (2014). La Privacidad en el Sistema Legal Chileno, p. 22. Santiago de Chile: Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/pp-08.pdf [Fecha de consulta: 04 de Junio, 2015].

11 Destaca la Constitución chilena como una de aquellas en Latinoamérica donde no existe reconocimiento expreso de la protección de los datos personales. Vd. Remolina, N. (2012). Aproximación constitucional de la protección de datos personales en Latinoamérica. Revista Internacional de Protección de Datos Personales vol. 1, n. 1. Bogotá: UDLA.

12 Remolina, N. 2012. Aproximación Constitucional de la Protección de Datos Personales en Latinoamérica. Revista Internacional de Protección de Datos Personales No. 1. En línea, disponible en: http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf [Fecha de consulta: 18 de noviembre, 2015]

13 Podemos señalar dos sentencias al respecto. En primer lugar, la sentencia STC N.º 389, en la cual se decidió que la atribución para recabar información sin limitación alguna violenta el derecho a la privacidad. Así, se argumenta que una habilitación en estos términos, sin trazar en la ley las pautas o parámetros que sean objetivos y controlables y que garanticen que el organismo se ha circunscrito a ellos, transgrede la privacidad, inviolabilidad de las comunicaciones y la dignidad humana.

Luego, la sentencia STC N.º 433 falló que la atribución del Ministerio Público para solicitar entrega de documentos sin limitación igualmente afecta al derecho a la privacidad, ello en tanto una habilitación para vulnerar este derecho no puede ser entregada a un organismo público sin reservas ni sin determinar pautas objetivas y sujetas a control vulnera el derecho a un procedimiento e investigación racionales y justos y vulnera en la esencia los derechos a la vida privada y reserva de comunicaciones privadas.

Ambas reseñas fueron extraídas de Carmona, C. y Navarro, E. (editores) (2011). "Recopilación de Jurisprudencia del Tribunal Constitucional (1981-2011)", pp. 191-192. Santiago: Tribunal Constitucional.

14 Corte Interamericana de Derechos Humanos. Caso Escher y Otros vs. Brasil, sentencia definitiva, 2009. http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf p. 34, párrafo 114. [Fecha de consulta: 04 de Junio, 2015].

15 Ibid., p. 35.

16 OEA. Corte Interamericana de Derechos Humanos. Tristán Donoso v Panamá, sentencia definitiva, 2009. p. 19, párrafo 56.

17 Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión, Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, Declaracion Conjunta Sobre Programas de Vigilancia y Su Impacto en La Libertad de Expresión: https://eff.org/r.973v [Fecha de consulta: 05 de Junio, 2015].

18 Nogueira, H 2004. "Pautas para Superar las Tensiones entre los Derechos a la Libertad de Opinión e Información y los Derechos a la Honra y la Vida Privada" en Rev. derecho (Valdivia) v.17 Valdivia diciembre de 2004. En línea, disponible en https://eff.org/r.4130 [Fecha de consulta: 14 de Junio, 2015].

19 Tribunal Constitucional de Chile (2010), "Requerimiento de parlamentarios y otros para que se declare la inconstitucionalidad del Movimiento Patria Nueva Sociedad". STC 567-06. Considerando 30º. En línea disponible en http://www.tribunalconstitucional.cl/wp/ver.php?id=1386 [Fecha de consulta: 14 de Junio, 2015]

20 García, G. y Contreras, P. (2014) Diccionario Constitucional Chileno. Santiago de Chile, Tribunal Constitucional de Chile, pp. 621-622.

21 Tribunal Constitucional de Chile (2010), "Requerimiento de parlamentarios y otros para que se declare la inconstitucionalidad del Movimiento Patria Nueva Sociedad". STC 567-06. Considerando 22º. En línea, disponible en http://www.tribunalconstitucional.cl/wp/ver.php?id=1386 [Fecha de consulta: 14 de Junio, 2015].

22 Carmona, C. y Navarro, E. op. cit., p. 178.

23 Silva, A. (2009). "El Derecho de Reunión en la Constitución de 1980. Temas Actuales de Derecho Constitucional, Libro Homenaje al Profesor Mario Verdugo Marinkovic", p. 305. Santiago: Jurídica.

24 García, G. y P. Contreras (2014). op. cit., op. cit., p. 334.

25 Ana Piquer, "¿Qué significa la ley Hinzpeter?", acuerdos.cl, https://eff.org/r.54wj [Fecha de consulta: 10 de Junio, 2015].

26 El Mostrador, "Vigilancia del gobierno a redes sociales trasciende fronteras y lo expone a ciberataque internacional", El Mostrador, 22 de junio de 2011. https://eff.org/r.zijh [Fecha de consulta: 10 de Junio, 2015].

27 Ciper Chile, "La polémica del monitoreo virtual", Ciper Chile, 22 de junio de 2011. http://ciperchile.cl/radar/la-polemica-del-monitoreo-virtual [Fecha de consulta: 10 de Junio, 2015].

28 Soy Chile, "La PDI aclaró que tiene un programa para espiar computadores, pero que lo usa con autorización judicial", Soy Chile, 06 de Julio de 2015. https://eff.org/r.54wj [Fecha de consulta: 06 de Julio, 2015].

29 Policía de Investigaciones de Chile, Jefatura Nacional de Asuntos Públicos, "Comunicado de Prensa". Santiago, 06 de julio de 2015. https://eff.org/r.gb5t [Fecha de consulta: 20 de Julio, 2015].

30 Partarrieu, B y Jara, M. "Los correos que alertaron sobre la compra del poderoso programa espía de la PDI", Ciper Chile, 10 de julio de 2015. https://eff.org/r.dwgm [Fecha de consulta: 20 de Julio, 2015].

31 Igualmente, nos remitimos a lo ya tratado en "La Privacidad en el Sistema Legal Chileno" pp. 70-73.

32 Ministerio de Transportes y Telecomunicaciones, Subsecretaría de Telecomunicaciones. Decreto 18 de 13 de febrero de 2014. "Aprueba Reglamento de Servicios de Telecomunicaciones que indica".

33 Ibid.

34 Lara, J, et al, op. cit., pp. 48-50. En línea, disponible en: https://www.derechosdigitales.org/wp-content/uploads/pp-08.pdf [Fecha de consulta: 09 de Julio, 2015].

35 "A person intercepts a communication in the course of its transmission if, as a result of his interference in the system or monitoring of the transmission, some or all of the contents are made available, while being transmitted, to a person other than the sender or the intended recipient of the communication" en Oxford University, "Legal Opinion on Intercept Communication" (2006). En línea, disponible en: https://eff.org/r.jzz3 p. 7 [Fecha de consulta: 09 de Julio, 2015].

36 Ministerio Público, Fiscalía Nacional del Ministerio Público. "Oficio N.º 060/2014 sobre Instrucción General que imparte criterios de actuación aplicables a la Etapa de Investigación en el Proceso Penal". Santiago de Chile, 23 de enero de 2014. p. 20.

37 Ibid., op. cit. p. 21.

38 La Segunda, "Golpe a la inteligencia policial: Fiscalía formalizará a ex oficial por escuchas ilegales". Urzúa, M y Candia, V, 16 de marzo de 2013.

39 Álvarez, D. y A. Cerda (2005). "Sobre la Inviolabilidad de las Comunicaciones Electrónicas. Ley Nº 19.927 que Tipifica los Delitos de Pornografía Infantil" en Anuario de Derechos Humanos 2005, p. 137. Santiago: Facultad

de Derecho, Universidad de Chile. En línea, disponible en: http://www.anuariocdh.uchile.cl/index.php/ADH/article/viewFile/13264/13539. [Fecha de consulta: 09 de julio, 2015].

40 La dirección IP considerada como dato personal no es algo universal, pues varía en los sistemas jurídicos alrededor del mundo. Dentro de los que las reconoce como tal es el caso español, siendo tal regulación de datos una que fuertemente influyó en la elaboración de la normativa chilena. Así, el año 2003 la Agencia Española de Protección de Datos (AEPD) emitió el informe denominado "Carácter de dato personal de la dirección IP. Informe 327/2003", documento en el cual se concluye que "aunque no siempre sea posible para todos los agentes de internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos". Este extracto puede encontrarse en Chaveli, E. "La Dirección IP, Problemas que Plantea", 2011. En línea, disponible en: http://www.gesdatos.com/wp-content/uploads/La-direcci%C3%B3n-IP.pdf [Fecha de consulta: 24 de septiembre, 2015].

La jurisprudencia de la Corte Interamericana de Derechos Humanos, en el ya citado caso Escher y otros v Brasil, entiende que la protección a las comunicaciones privadas no solamente cubre al contenido mismo sino que también a los metadatos asociados a aquellas. Por tanto, cualquier tipo de comunicación llevada a cabo a través de internet, según esta sentencia de la Corte, goza de protección al igual que la dirección IP del equipo usado para su emisión. Considerando que Chile ha reconocido la competencia de este órgano jurisdiccional internacional y la construcción intelectual del "control de convencionalidad" elaborada por la Corte IDH, tanto el articulado de la Convención Interamericana de Derechos Humanos como la interpretación de la misma son directamente vinculantes para los Estados parte. Cfr. Hitters, J. "¿Son vinculantes los pronunciamientos de la Comisión y de la Corte Interamericana de Derechos Humanos? (control de constitucionalidad y convencionalidad)" en Revista Iberoamericana de Derecho Procesal Constitucional, número 10, julio-diciembre 2008, pp. 131-156.

41 Ver nota 38.

42 Chile, 1979. Ministerio de Defensa Nacional. Decreto Ley N.º 2.460 "Ley Orgánica de la Policía de Investigaciones de Chile".

43 Chile, 1990. Ministerio de Defensa Nacional. Ley N.º 18,691 "Ley Orgánica Constitucional de Carabineros".

44 Morelos, J. "¿Qué es Hacking Team y su herramienta DaVinci?", luisgyg.com, 07 de julio de 2015. http://www.luisgyg.com/blog/2015/07/07/que-es-hacking-team [Fecha de consulta: 20 de Julio, 2015].

45 Policía de Investigaciones de Chile, Jefatura Nacional de Asuntos Públicos, "Comunicado de Prensa". Santiago, 06 de julio de 2015. https://pbs.twimg.com/media/CJQdW9KW8AEg9Rl.jpg [Fecha de consulta: 20 de Julio, 2015].

46 El Mostrador, "Diputados se reúnen con Director de la PDI para que explique compra de software de espionaje", 22 de julio de 2015. El Mostrador. En línea, disponible en: http://www.elmostrador.cl/noticias/pais/2015/07/22/diputados-se-reunen-con-director-de-la-pdi-para-que-explique-compra-de-software-de-espionaje/ [Fecha de consulta: 22 de febrero de 2016]

47 Ibid.

48 Ver nota 43.

49 Peña, P. y F. Vera (2014). "Derecho a protesta y vigilancia policial en redes sociales", Digital Rights Lac, 30 de junio de 2014. En línea, disponible en: http://www.digitalrightslac.net/es/derecho-a-protesta-y-vigilancia-policial-en-redes-sociales [Fecha de consulta: 20 de Julio, 2015].

50 OEA, ONU. "Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión", 21 de junio de 2013. En línea, disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927 [Fecha de consulta: 20 de Julio, 2015].

51 INDH. "Informe sobre cuestiones a considerar en una reforma de la Ley Antiterrorista a la luz de la observación de casos realizada por el Instituto Nacional de Derechos Humanos". Aprobado por el Consejo del Instituto Nacional de Derechos Humanos el 22 de julio de 2014. pp. 4-7. En línea, disponible en: http://bibliotecadigital.indh.cl/bitstream/handle/123456789/655/Informe%20Ley%20Antiterrorista.pdf?sequence=1 [Fecha de consulta: 24 de Junio, 2015]

52 Ibid., p. 7.

53 Naciones Unidas. Derechos Humanos: "Declaración del Relator Especial de las Naciones Unidas sobre la promoción y la protección de los derechos humanos y libertades fundamentales en la lucha contra el terrorismo", ohchr.org, 30 de julio de 2013. En línea, disponible en: http://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=13598 [Fecha de consulta: 24 de Junio, 2015].

54 Lara et al., op. cit. pp. 63-69

55 Sentencia "Caso Bombas" R.I.T. N.º 138-2011, R.U.C N.º 0700277303-6.

56 Senado de la República, Departamento de Prensa. "Director de la ANI expuso en sesión secreta sobre situación de La Araucanía". Disponible en: https://eff.org/r.p7np

57 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/text; EFF, ARTICLE19, Análisis Jurídico Internacional de Apoyo y Antecendentes de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/AnalisisLegal; Access, Guía Universal de Implementación de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://eff.org/r.4gac [Fecha de consulta: 20 de Julio, 2015].

58 FayerWayer, "Chile: Derechos Digitales denuncia a la Policía de Investigaciones por no respetar la vida privada", 26 de abril de 2012. https://eff.org/r.z6r1

59 El informe anual de Twitter puede encontrarse en: https://transparency.twitter.com/country/cl [Fecha de consulta: 24 de septiembre, 2015] y el informe de Facebook en: https://govtrequests.facebook.com/country/Chile/2014-H2/ [Fecha de consulta: 24 de septiembre, 2015].

60 OEA, "Inter-American Convention on Mutual Assistance in Criminal Matters", 1992. http://www.oas.org/juridico/english/treaties/a-55.html [Fecha de consulta: 22 de julio, 2015].

61 FayerWayer, "Chile: Formalizan a abogado por crear una cuenta de parodia en Twitter del empresario Andrónico Luksic", 19 de febrero de 2013. https://eff.org/r.2lnm

62 Ruiz, C. (2014). " Sobreseimiento definitivo en causa de Luksic versus parodia en Twitter". https://eff.org/r.rhzq

63 Cámara de Diputados Chile, Boletín Nº 9243-10 "Aprueba el Acuerdo entre el Gobierno de Chile y el Gobierno de los Estados Unidos de América en materia de incremento de la cooperación en la prevención y combate del delito grave suscrito en Washington, D.C", 20 de mayo de 2013. http://www.camara.cl/sala/verComunicacion.aspx?comuid=10784&formato=pdf [Fecha de consulta: 22 de Julio, 2015].

64 Lara, J, Martínez, M y Viollier, P (2014). "Hacia una regulación de los delitos informáticos basada en la evidencia", en Revista Chilena de Derecho y Tecnología (2014), pp. 106-107.

65 United Nations, op. cit.