Universidad de Chile
Facultad de Derecho
Departamento de Derecho Público

Derecho a la privacidad y vigilancia masiva

Memoria para optar al grado de Licenciada en Ciencias Jurídicas y Sociales

Consuelo Osorio Vargas

Santiago, Chile

2018

Profesor guía: Dr. iur. utr. Teodoro Ribera Neumann

AGRADECIMIENTOS

A mis padres y hermana, por su apoyo y cariño incondicional durante todo este proceso.

A mis abuelos, Luis y Eva, por su preocupación, cariño y fortaleza.

A toda mi familia Vargas por siempre creer en mí.

A mis amigas por el constante apoyo y preocupación.

ÍNDICE

RESUMEN

Reconociendo la importancia de actualizar las herramientas que los servicios de inteligencia cuentan para llevar a cabo su labor, este trabajo tratará una de las más controvertidas, la vigilancia masiva, y en específico, su interacción con el derecho a la privacidad. Así, se comenzará por analizar en que consiste esta, su alcance y uso en la actualidad. Su intrínseca relación con los derechos humanos será analizada a la luz de las posibles afectaciones que puedan estos sufrir.

Para determinar las exigencias bajo las cuales puede permitirse la vigilancia masiva, se tratará su régimen a nivel internacional, ya sea por medio de legislación comparada o por los pronunciamientos recaídos por parte de organismos internacionales. El objetivo final, será determinar los estándares que esta actividad debe cumplir en caso de ser utilizada a nivel nacional. Su falta de tratamiento a nivel nacional, requerirá examinar la normativa que en la actualidad permite la interceptación de las comunicaciones, y en base a esta construir esta respuesta.

Palabras clave: vigilancia masiva, privacidad, derechos humanos, interceptación de comunicaciones.

ABSTRACT

Recognizing the importance of updating the tools that intelligence services have to carry out their work, this work will deal with one of the most controversial, massive surveillance, and specifically, its interaction with the right to privacy. Thus, it will begin by analyzing what it is, its scope and current use. Its intrinsic relationship with human rights will be analyzed in light of the possible effects that these suffer.

In order to determine the requirements under which mass surveillance can be allowed, its regime will be treated at an international level, either through comparative legislation or by pronouncements handed down by international organizations. The final objective will be to determine the standards that this activity must meet if it is used nationally. Its lack of treatment at the national level, will require examining the regulations that currently allow the interception of communications, and based on this build this response.

Key words: mass surveillance, privacy, human rights, interception of communications.

INTRODUCCIÓN

La revolución tecnológica de las últimas décadas, la cual ha importado una serie de avances jamás pensados, ha exigido repensar el paradigma bajo el cual los derechos humanos son entendidos. Las amenazas a estos han evolucionado, se han vuelto más sofisticadas e impredecibles, requiriendo de un nuevo marco normativo que se adapte y pueda entregar las garantías y protección que la sociedad contemporánea exige.

El terrorismo y el crimen organizado, considerados como unas de las grandes amenazas que aterran e inquietan a la población en general, de igual forma han reclamado replantear las herramientas utilizadas para combatirlos. Eventos como el ocurrido el 11 de septiembre de 2001 en el World Trade Center, o más recientemente, el atentado en el Manchester Arena en 2017, han generado un contexto de peligro constante, de amenaza sin precedente.

Múltiples soluciones han sido erigidas, pero la necesidad de conciliar la persecución del delito con su integración con la tecnológica ha derivado en soluciones altamente intrusivas y poderosas. El desarrollo y expansión de la biometría es una muestra de esto, así como la televigilancia y la vigilancia masiva. Todas tienen en común una incipiente regulación, y la tendencia por superponer los intereses de seguridad en desmedro de las consideraciones concernientes a los derechos humanos que afectan.

A su vez, las formas en que las personas se comunican han evolucionado drásticamente, la irrupción del teléfono celular, smartphones, computadores portátiles, redes sociales, entre otros, han significado un cambio en el paradigma bajo el cual se entiende la interacción humana. Esto ha derivado en que gran parte de la información de mayor importancia dentro de la vida de una persona se encuentre contenida en medios que han abandonado lo físico, existiendo solo en un plano digital. Aún más, esta información no solo deriva de aquello que expresamente las personas exponen, comparten o guardan en estas plataformas, incluyen, además datos asociados o vinculados como la localización satelital o GPS. En efecto, la información y datos recopilados y almacenados online o en aparatos tecnológicos, excede lo que las personas comunes y corrientes, legos en la materia, puedan imaginar.

El derecho a la privacidad por su parte, desde su concepción más primitiva ha estado a merced de los cambios generados en la sociedad en la cual se encuentra inmersa. Se

presenta como un reflejo de las necesidades propias de una sociedad en constante evolución, la cual impone desafíos constantes para asegurar su protección adecuada. Desde su desarrollo más primitivo relacionada al mero aislamiento, hasta su moderno desarrollo el cual contempla el control que los sujetos poseen respecto de su información, esta ha debido adaptarse. Ya las exigencias impuestas por el solitario hombre medieval sediento de un lugar de refugio y aislamiento, han sido superadas, requiriendo en la actualidad su comprensión y desarrollo en atención a las necesidades impuestas por una sociedad tecnológica, altamente interconectada e indecisa respecto de que es aquello que pretende resguardar.

Es en este contexto de interacción entre tecnología y derechos humanos, es que la vigilancia masiva se inserta. Esta, a diferencia de cualquier otro tipo de vigilancia conocida, se caracteriza fundamentalmente por su enorme potencial lesivo, el cual se encuentra determinado por dos características esenciales: su masividad y acceso ilimitado a las plataformas y aparatos intervenidos. La masividad, en el contexto de la sociedad tecnológica, dice relación con la potencialidad que esta posee para afectar a la población. Su desarrollo alcanza a todas las personas, a la población en su totalidad. Este amplio alcance solo es limitado por la falta de acceso a aparatos, servicios o plataformas tecnológicas, sin importar su calidad de abierta o cerrada.

El acceso ilimitado que proporciona la vigilancia masiva importa un potencial indiscriminado para ingresar, conocer y procesar la información existente en los aparatos o plataformas utilizados por la población. Las posibilidades son vastas e incalculables. El conocimiento del contenido de la información, es solo la versión básica y regular de este tipo de actividad.

Bien podría pensarse que ante semejante amenaza existiría alguna forma de resguardo que impida dicha intromisión, lo cual, si bien es cierto, es prácticamente imposible. La vigilancia masiva utiliza cada plataforma web o digital conocida, aparatos inteligentes y computadoras, entre otros, para acceder y apropiarse de la información generada en estos. La abstención de estos medios en el contexto de la vida moderna es imposible, pues significaría convertirnos en parias sociales, sin contacto con el mundo.

Impedir el desarrollo de esta actividad si bien es posible, requiere de un gran sacrificio que en realidad no es necesario ni debería ser una opción tomar.

Es así como la respuesta a esta problemática no se encuentra en abogar por su erradicación, sino que, por el contrario, en su control. En el establecimiento de exigencias, limitaciones y pautas de control que permitan minimizar el daño provocado por esta actividad. La pregunta que debemos hacernos no es ¿Cómo erradicar la vigilancia masiva?, sino que, por el contrario, ¿Cuáles son sus supuestos de procedencia?, ¿Qué alcance debe tener el control judicial respecto de ella?, ¿Qué garantías procesales se otorgaran a las personas afectadas por estas?, ¿Cuál será su extensión e incidencia en respecto de las comunicaciones de los afectados?, y en definitiva, ¿De qué forma será esta conciliada con el respeto irrestricto con los derechos humanos?

El peligro que reside en este tipo de actividades no es tan simple y burdo, como podría pensarse; lo que está en juego no es que una computadora pueda espiar una conversación vía Facebook, o "robar" una imagen almacenada en la nube. El riesgo al cual nos vemos expuestos es mucho más sofisticado y complejo, y radica en el control que cada una de las personas posee sobre su información, la cual puede ser extraída sin problema alguno por el Estado que dice protegerlos, obteniendo por medio de ésta una serie de conclusiones respecto de sus vidas, que tornaría el derecho a la privacidad como un mero recuerdo del pasado.

La problemática se centra en el establecer un nuevo límite entre lo público y lo privado, que lo permitido y lo prohibido el derecho.

CAPITULO I: VIGILANCIA MASIVA Y EL DERECHO A LA PRIVACIDAD

1.1 Concepto vigilancia masiva

Es necesario iniciar el estudio del tema en cuestión estableciendo que se entenderá por vigilancia masiva, actividad que si bien ha adquirido una especial relevancia en los últimos años, no ha sido tratada con profundidad en el medio nacional o regional.

La vigilancia masiva puede ser conceptualizada como "aquel monitoreo sistemático, es decir, que se realiza de forma constante o por un periodo de tiempo determinado, dirigida a grandes grupos de usuarios de internet -por ello es masiva-, quienes al comunicarse o interactuar mediante plataformas web generan distintos tipo de información que son recopiladas, almacenados y eventualmente analizados para determinar actos, conductas, preferencias, localización y otras características que permitan individualizar a los usuarios."[1] A pesar de que dicha definición comprende gran parte de las actividades que componen la vigilancia masiva, esta excluye aquellas llevadas a cabo por medio de la interceptación, grabación y retención de las comunicaciones telefónicas.

Comprende una forma de "vigilancia estratégica", en oposición de la tradicional vigilancia dirigida, diferenciándose de esta última en la falta de sospecha determinada respecto de la población afectada por ella. Es por esta consideración que se ha estimado que un elemento característico de la vigilancia masiva es la proactividad, en cuanto su objetivo no es perseguir a un sujeto en particular previamente considerado como sospechoso, sino que, por el contrario, pretende identificar producto del análisis de toda la población, quien es el sujeto sospechoso.[2]

[1] Rayman Labrín, Danny. (2015). Chile: Vigilancia y el derecho a la privacidad en internet. Revista Chilena de Derecho y Tecnología, Chile, Vol. 4 (1): 206. p.206.

[2] Council of Europe, Mass Surveillance. (2017). [en línea] Disponible en <https://rm.coe.int/factsheet-on-mass-surveillance-corrected-and-final-rev2august2017/1680736031Thematic factsheet1> [Consultado el 20 de septiembre de 2018]

Para ilustrar las distintas etapas como procesos que conlleva el desarrollo de esta actividad, se utilizara la taxonomía de la privacidad desarrollada por Daniel Solove, la cual permite exhibir y comprender la extensión y peligro que conlleva la vigilancia masiva.

La primera fase, comprende el monitoreo sistemático de la actividad de las personas en línea, por un periodo indeterminado de tiempo. Se concentran en esta etapa todas aquellas labores tendientes a la recopilación tanto de información como de datos, desarrollándose por consiguiente la labor misma de vigilancia.[3] La vigilancia en este contexto se compone de una serie de tareas tales como la observación, la escucha y/o el registro de la actividad de un individuo.[4] La recopilación de la información permite la obtención de cualquier dato susceptible de ser interceptado, comprendiendo la captación de correos electrónicos, contraseñas, fotografías, llamadas de voz e imagen, actividad en las redes sociales, contraseñas y otros datos de los usuarios de internet,[5]así como todo registro de la actividad en línea."[6]

Una característica esencial de esta etapa es la falta de conocimiento por parte del sujeto vigilado, de que dichas actividades están siendo llevadas a cabo. Consecuencial a este desconocimiento es el alto poder intrusivo que estos métodos ofrecen, otorgando acceso a toda clase de información, sin que una selección previa sea necesaria o relevante.[7]

Un aspecto determinante de esta primera etapa, consiste en que la sola irrupción en las formas de almacenamiento de información resulta atentatoria a los derechos fundamentales

[3] Solove J, Daniel. (2006). A taxonomy of privacy. [en línea]. Disponible en <p.490https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477.pdf> [Consultado el 18 de junio de 2018] p.490.

[4] Ídem.

[5] Garriga Domínguez, Ana. (2016). Nuevos retos para la Protección de Datos Personales. En la Era del Big Data y la Información Oblicua. [en línea], Madrid, Dykinson. Disponible en <https://app.vlex.com/#WW/sources/14328> [Consultado el 30 de marzo]. p. 46.

[6] Parlamento Europeo, Informe sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos de Interior, 21 de febrero de 2014. [en línea] Disponible en <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//ES#title2> [Consultado el 17 de abril de 2018]

[7] Barinas Ubiña, Désirée. 2013. El Impacto de las Tecnologías de la Información y de la Comunicación en el Derecho a la Vida Privada: Las Nuevas Formas de Ataque a la Vida Privada. Revista Electrónica de Ciencia Penal y Criminología. [en línea] N° 15 Disponible en < https://dialnet.unirioja.es/servlet/articulo?codigo=4407594 > [Consultado el 15 de junio de 2018] p.12.

de la población.[8] Esto, en consideración de que tan solo el mero acceso a dichos datos, sin importar su posterior uso, significa una vulneración al espacio protegido por el derecho a la privacidad.

La indefinición de las personas se presenta como una característica fundamental de la actividad, produciéndose un monitoreo indiscriminado que intercepta las comunicaciones de forma aleatoria, sin que existan criterios que reduzcan la población objetiva.[9] Es además inherente a la actividad, que la susceptibilidad de la población afectada radique en el uso de cualquier plataforma online u aparato tecnológico, que permita obtener algún tipo de registro, apto para el tratamiento que implica la vigilancia.

La segunda etapa de la vigilancia masiva es aquella destinada al procesamiento de la información. Esta etapa comprende todas aquellas actividades tendientes al procesamiento de la información, entendiendo como parte de este el uso, almacenamiento y manipulación de todo aquello recolectado en la etapa precedente.[10] Este procesamiento de información puede tomar una serie de formas dependiendo del tratamiento al cual se someta a la información, siendo relevantes a este respecto la agregación e identificación.

La agregación entendida desde la perspectiva del procesamiento de información, consiste en la recopilación y conexión de toda la información que se ha obtenido de una persona por medio de los procesos de vigilancia.[11] Un factor fundamental para llevar a cabo esta tarea es la digitalización, la cual permite la gestión y coordinación de un sistema altamente complejo, disperso, descentralizado y desorganizado, otorgando una forma de lenguaje universal que permite establecer la comunicación entre las distintas bases de datos consultadas.[12]

---

[8] J. Solove, Daniel. (2008). Understanding Privacy, Harvard University Press. GWU Legal Studies Research Paper N° 420, p. 106

[9] Informe Sobre la Existencia de un Sistema Mundial de Interceptación de Comunicaciones Privadas y Económicas, de 11 de junio de 2001 [en línea] Disponible en <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//ES> [Consultado el 17 de abril del 2018]

[10] Solove J, Daniel. A Taxonomy of Privacy. op. cit. p. 508.

[11] Solove J, Daniel. ibid p. 506.

[12] Whitaker, Reg. (1999) El fin de la privacidad: Cómo la vigilancia total se está convirtiendo en realidad. The New Press, Nueva York. p. 154.

Esta actividad permite además relacionar información aparentemente inconexa e inservible, transformándola en una fuente de datos completa de la persona o población en cuestión, otorgando un conocimiento acabado en múltiples áreas de su vida. Por medio de ésta se incrementa exponencialmente el valor de la información individualmente considerada.[13]

Este procesamiento, al igual que la vigilancia, es una manera de adquirir información sobre la población. Sin embargo es una de naturaleza indirecta o secundaria, toda vez que esta toma lugar cuando la información ya ha sido obtenida, solo operando respecto del análisis de esta, y no en la etapa de recolección misma.[14] La particularidad de esta forma de obtención de datos, en atención a su carácter secundario, es que permite arribar a conclusiones o determinar cuestiones complejas que la información en un estado básico no permitiría. Por medio de este proceso se logra la coincidencia y vinculación de datos que, en definitiva, produce información nueva y valiosa, no tan solo desde una perspectiva de inteligencia y seguridad nacional, sino que también desde un punto de vista comercial.[15]

De vital importancia en el proceso de agregación es el creciente desarrollo tecnológico, el cual ha permitido que este se implemente procesos altamente sofisticados, que son capaces de analizar una gran cantidad de datos en un corto periodo de tiempo o incluso de forma automática.

Por su parte, la identificación, es entendida como aquel proceso por medio del cual se vincula la información obtenida con un sujeto determinado, es decir, se verifica la identidad de la persona de la cual se ha obtenido esta.[16] La importancia de la identificación radica en que permite establecer la identidad del sujeto vigilado, además de en determinados casos individualizar al sospechoso de la comisión de un delito.[17] Relevantes a este respecto son las bases de datos, las cuales por medio de sofisticados análisis facilitan la recopilación

[13] Idem.
[14] Solove J, Daniel A Taxonomy of Privacy. op. cit. p.507.
[15] Whitaker. op. cit. p. 154.
[16] Solove J, Daniel. A Taxonomy of Privacy. op. cit. p.510.
[17] Ídem.

cruzada de datos, permitiendo la obtención de un perfil acabado de toda la información disponible de un sujeto en determinado.[18]

La agregación, en conjunto con la identificación, posibilita relacionar aquellos patrones y conductas, gustos o cualquier otro tipo de información reunida, con un sujeto en específico, respecto del cual se han llevado a cabo las actividades de vigilancia masiva.

De la consideración en conjunto de ambas labores es que se deriva el peligro de la vigilancia masiva, la cual, como lo ha señalado el Tribunal de Justicia de la Unión Europea, "pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuenta."[19]

En este punto debe precisar que se entenderá por información y datos, toda vez que de esta consideración permite establecer la extensión que la vigilancia puede alcanzar. Información ha sido entendida por la Real Academia Española como aquella "comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen de una materia determinada". Datos en cambio, es concebido como aquella "información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivas de un hecho." Una comprensión más acabada de información permite conceptualizarla como " un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones."[20]

[18] Whitaker op. cit. p.154.
[19] Tribunal de Justicia de la Unión Europea, C-293/12 - Digital Rights Ireland y Seitlinger y Otros, de 8 de abril de 2014. Apartado 24.
[20]Chiavenato, Idalberto. (2006) Introducción a la Teoría General de la Administración», Séptima Edición, México, McGraw-Hill Interamericana, p.110.

Enseguida, una especial y relevante clasificación a la cual debe hacerse mención, es aquella referente a los denominados datos sensibles, que si bien han sido definidos por nuestra legislación nacional[21], comprenden una subcategoría de los datos personales que al igual que estos últimos se encuentra amparado por el derecho a la privacidad, pero a diferencia de estos requieren de una especial protección.[22]

Dichos datos comprenden aquella "información sobre la vida sexual, conyugal o doméstica, los defectos físicos o los rasgos psíquicos, el grupo sanguíneo, el credo religioso y la filiación política, la educación de los hijos y, ahora, el código genético del individuo y su familia."[23]

Los datos sensibles, como expresión de los datos personales, exigen de una especial protección, inclusive mayor a la reconocida a estos últimos. Esta consideración se basa en el potencial lesivo estos detentan, lo que cual deriva en que tanto objetiva como subjetivamente, el daño sufrido en caso de transgresión sea sustancialmente mayor y pernicioso.[24] Consecuencia directa de la relevancia de estos datos es que pueden ser utilizados en desmedro de su titular, en virtud de lo cual se ha estimado que "Estos no pueden ser nunca, en circunstancia, por causa o finalidad alguna, colocados en la situación de ser difundidos sobre la base de invocar un interés social, público o supraindividual."[25]

La importancia de distinguir entre esta serie de clasificaciones de datos, radica en que, a pesar de que pueda existir una expectativa legitima y fundada de acceder a todos ellos, la determinación de estos como datos sensibles, los excluye del conocimiento y divulgación de forma total por parte del aparato estatal. La sola consideración de la importancia de que

[21] Datos sensibles: aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

[22]Quezada Rodríguez, Flavio. (2014). La protección de datos personales en la jurisprudencia del Tribunal Constitucional. Revista de Derecho Público, (76), Págs. 425-441 p. 436.

[23] Cea Egaña, José Luis, (2000). Los Derechos a la Intimidad y a la Honra en Chile. Ius et Praxis. [en línea] Disponible en <http://www.redalyc.org/articulo.oa?id=19760208> ISSN 0717-2877 [Consultado el 21 de septiembre de 2018]. p.159.

[24] Quezada Rodríguez, F. op. cit. p.437.

[25] Cea Egaña, Luis. op. cit. p.159.

dichos datos revisten, importa que sólo el sujeto titular de estos se encuentra autorizado para permitir su revelación, de forma voluntaria y en consideración de la confidencialidad que se entiende es parte de estos.[26]

Sin embargo, la protección genérica de los datos sensibles no sería del todo suficiente, toda vez que, en concordancia con lo previamente expuesto, como resultado de los procesos de agregación e identificación se puede llegar a obtener datos sensibles de otros que no revisten el carácter de tal.[27] Si bien en abstracto la delimitación entre los datos sensibles y el resto es clara, al considerar los métodos de vigilancia y procesamiento de información, este límite se desdibuja hasta desaparecer, ya que al existir la posibilidad de acceder a estos de forma indirecta, importa que su titular pierda el control natural que posee respecto de ellos.

La tercera y última etapa, está destinada naturalmente a la utilización de la información recopilada. El empleo de la información es infinito y depende de los objetivos que se persigan por parte de las agencias que han recopilado la información, así como los impuestos por los Estados. A pesar de que la información o datos tratados puedan estar dirigidos a un uso en particular, la importancia que esta posee puede acarrear la ocurrencia de una serie de atentados contra la privacidad, consistentes en la amenaza de revelación o divulgación esta.

Este grupo se ha determinado en atención a una serie de acciones descritas por Daniel Solove, siendo estas las denominadas, (1) brecha de confidencialidad, (2) divulgación, (3) exposición, (4) accesibilidad incrementada, (5) extorsión, (6) apropiación y (7) falseamiento o tergiversación.[28]

Para el objeto del trabajo en cuestión, nos centraremos en la divulgación, dado que dichas amenazas revisten la mayor preocupación respecto del desarrollo de actividades de vigilancia masiva. La divulgación tiene por objeto la publicación de asuntos personales de

[26] Pfeiffer, María Luisa. (2008). Derecho a la privacidad. Protección de los datos sensibles. Revista Colombiana de Bioética [en línea], Disponible en: <http://www.redalyc.org/articulo.oa?id=189217248002> [Consultado el 20 de noviembre de 2018] p.27.
[27] Pfeiffer, María Luisa ibid. p.26.

una persona usualmente protegidos por la ley.[29]Esta forma de amenaza a la privacidad, se vincula con los previamente mencionados datos sensibles o cualquier otro que en su particularidad revista de alguna importancia para el sujeto. Uno de los grandes peligros que se producen al divulgar esta información clasificada, queda de manifiesto, por ejemplo, en la publicación de la dirección de un testigo protegido.[30]

1.2 El desarrollo de la vigilancia masiva con las nuevas tecnologías

La vigilancia masiva tal y como es concebida en la actualidad, no es un fenómeno reciente, sino que se presenta como el producto de la evolución de una serie de prácticas realizadas a lo largo de la historia por parte de entidades estatales, con el objeto de conocer información considerada como privada. El avance tecnológico es de gran relevancia en la materia, toda vez que, si bien permite el desarrollo de nuevos medios de intercambio y almacenamiento de información, hace posible en directa relación la creación de tecnología que haga factible el acceso a dicha información.

El desarrollo de las técnicas de vigilancia, además de ser fruto del desarrollo tecnológico de las últimas décadas, es el resultado de un cambio en el paradigma bajo la cual esta es concebida. Se pasa de una concepción de vigilancia reactiva, a una de naturaleza proactiva. Ya no es necesario la concretización de la amenaza para que esta tome lugar, ya que, la vigilancia se transforma en una práctica común y generalizada, la cual amplía su objetivo de la sola observación y monitoreo constante, a la comparación del actuar observado con un patrón "socialmente aceptable" o "sospechoso", del cual se deriva la peligrosidad de la población observada.[31]

La clave para comprender la actual forma que ha adquirido la vigilancia masiva es la digitalización de las comunicaciones y de toda interacción personal llevada a cabo en línea. Esta ha permitido la creación de un lenguaje y plataforma de almacenamiento universal de la información, la cual facilita el flujo de datos de una forma simplificada, que si bien se

[29] Solove, Daniel J. A Taxonomy of Privacy. op. cit. p. 529.
[30] Solove, Daniel J. ibid. p.530.
[31] Barinas, Désirée. op. cit. p.6.

orienta a la población usuaria, permite de igual forma que su interceptación se produzca a mayor escala y frecuencia. .[32]

El desarrollo de estas prácticas, se condice con la necesidad por parte de los estados de obtener información que pueda contribuir al resguardo de la seguridad nacional, como el combate en contra de toda forma de crimen organizado. En este entendido "las comunicaciones representan una valiosa fuente de datos que el Estado puede utilizar para prevenir o enjuiciar delitos graves o evitar posibles emergencias de seguridad nacional."[33]

Históricamente se puede reconducir el origen de la vigilancia masiva al UKUSA Agrement[34] firmado en la década de 1940 entre Estados Unidos de Norteamérica y el Reino Unido de Inglaterra e Irlanda del Norte, integrándose a este tiempo después Australia, Nueva Zelanda y Canadá. Su objetivo era desarrollar una red cooperación internacional en el contexto de la Segunda Guerra Mundial. Con el término de la guerra, pero dentro del contexto de la Guerra Fría, se creó el programa de vigilancia "ECHELON", el cual tenía por objetivo interceptar las comunicaciones entre la Unión Soviética y sus aliados.

En cuanto a su funcionamiento, ECHELON permitía la interceptación de todo tipo mensaje, fuera este enviado por fax, teléfono, Internet o e-mail, con independencia de su remitente, lo que era posible gracias a las diversas estaciones de interceptación de comunicaciones creadas para estos efectos.[35]

ECHELON constituye bajo este entendido, de acuerdo con lo señalado por Perez Luño, un "sistema que funciona a escala mundial gracias a la colaboración e interacción de los Estados (…), lo cual posibilita una vigilancia a nivel mundial de las comunicaciones por

[32] Whitaker op. cit. p.154.
[33]Organización de las Naciones Unidas, Asamblea General. "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue" Resolución A/HRC23/40, [en línea] Disponible en <https://undocs.org/es/A/HRC/23/40> [Consultado el 26 de noviembre de 18]
[34] Consultar los archivos desclasificados por la Agencia Nacional de Seguridad de Estados Unidos de Norteamérica en < https://www.nsa.gov/news-features/declassified-documents/ukusa/>
[35] Pérez Luño, Antonio. (2002) Internet y los Derechos Humanos Anuario de Derechos Humanos. Nueva Época. Vol. 2, págs. 101-121. p. 107.

satélite. Poniendo en común iniciativas, recursos técnicos y lógicos, costes y objetivos, representando una implacable y completa red de control a escala planetaria."[36]

En cuanto a su estado actual, este fue por primera vez revelado realizadas por Edward Snowden, un ex analista de la Agencia Nacional de Seguridad de Estados Unidos de Norteamérica, el cual expuso el desarrollo de prácticas efectuadas por el Gobierno de Estados Unidos en materia de inteligencia. Por medio de estas, quedaron al descubierto una serie de actividades constitutivas de espionaje masivo, las cuales afectaban no tan solo a ciudadanos norteamericanos, sino que se hacían extensibles a múltiples Estados europeos y americanos, incluyendo a algunos mandatarios de estos países.[37]

Superada la primera etapa que da origen a las actividades de vigilancia masiva, esta comienza a ser utilizada a nivel doméstico por medio de la interceptación de comunicaciones. Estas actividades que toman lugar en la década de 1970 tenían por objeto la interceptación de las llamadas telefónicas, por medio de la colocación de dispositivos de interceptación en los cables telefónicos, los cuales permitían escuchar las llamadas realizadas a través de este.[38]

En este periodo las amenazas a la privacidad se circunscriben a los dispositivos de escucha de conversaciones, sean estas realizadas a distancia o de forma presencial. Esta forma de vigilancia tiene directa relación con el avance tecnológico de la época, el cual se caracterizaba en aquel momento por la expansión del uso del teléfono a nivel domiciliario, restringiendo exclusivamente a las llamadas telefónicas y su contenido a las actividades de vigilancia. La evolución en el área de las comunicaciones por medio de la sustitución de las redes telefónicas analógicas por fibra óptica, en la década de 1990, derivó en la necesidad del rediseño de la tecnología para permitir la interceptación orientada a la vigilancia, de tal modo de que se pudiera acceder y controlar de forma remota las redes telefónicas.[39]

[36] Ídem.
[37]The Guardian. Edward Snowden and the NSA-time files [en línea] Disponible en <https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline> [Consultado el 26 de noviembre de 2018]
[38] La Rue, Frank. op. cit. p. 5.
[39] Ídem.

De forma paralela se comenzaron a rediseñar las actividades de vigilancia por medio de la captura de registros audiovisuales, conocidos como videovigilancia. Estas en sus inicios no permitían una imagen y sonido de calidad, evolucionando posteriormente de una imagen analógica de baja calidad, a una digital que, dependiendo de las características en particular, otorga una imagen de alta resolución que permite distinguir una serie de detalles contenidos en la imagen. Este progreso ha incidido, además, en el tamaño y apariencia de los objetos ocupados para estos efectos, los cuales en sus orígenes se caracterizaban por su gran tamaño y fácil identificación. En la actualidad estos aparatos son de un tamaño reducido, pudiendo fácilmente ser camuflados en los lugares en que se encuentran, volviéndose imperceptibles.[40]

Se han introducido además, igualmente aparatos fotográficos que permiten la captura de imágenes y videos infrarrojos a amplia distancia, como nuevas formas de vigilancia. [41]

La vigilancia masiva también ha hecho suya ciertos avances tecnológicos como la geolocalización, también conocida como GPS (Global Positioning System). Por medio de esta nueva herramienta, la cual en sus orígenes fue diseñada para el uso militar, se permite localizar a una persona u objeto con una margen de error de entre 30 y 50 metros (para fines civiles), en cualquier parte del mundo, además de seguir y registrar todos sus desplazamientos.[42] En cuanto a la tecnología orientada a la vigilancia masiva, su uso en teléfonos celulares permite conocer la ubicación exacta del sujeto usuario de este en todo momento, información que es almacenada por los proveedores de estos servicios así como cualquier tercero que pueda intervenir el aparato,[43] permitiendo mantener un registro actualizado de los desplazamientos de la población afectada.

En este contexto de constante desarrollo se produce la creación y desarrollo de internet, el que encuentra su origen en el ARPANET o Advanced Research Project Agency, creado por el Departamento de Defensa de los Estados Unidos, el cual tenía por objeto transmitir correos electrónicos. La particularidad de este nuevo medio de comunicación radicaba en

[40]La Rue, Fran. ibid. p.6.
[41] Ídem.
[42] La Rue, Frank ibid. p. 8.
[43] La Rue, Frank ibid. p. 9.

que podía continuar su funcionamiento incluso cuando una de las partes de la comunicación fuera destruida.[44] Su masificación se produjo en la década de 1990, resultando no tan sólo en una revolución en la forma en que se llevaban a cabo los intercambios comunicacionales de las personas, sino que además, en la transformación de la forma en las cuales se llevaban a cabo las actividades de vigilancia masiva.

Internet permitió un cambio radical en la forma en que se genera e intercambia la información la instantaneidad en todos los procesos en que esta se involucra derivó en un esfuerzo por parte de los Estados por acceder a esta. Al facilitar la elaboración de un gran volumen de datos de comunicaciones o metadatos, por medio de toda interacción o actividad desarrollada en la web, ha generado el espacio para que estos sean potencialmente recopilados, almacenados y tratados, toda vez que estos son fácilmente accesibles.[45]

En la actualidad el solo acceso a una computadora permite potencialmente ser objeto de vigilancia, en tanto se puede acceder a todos los archivos creados y gestionados en este, así como toda actividad llevada a cabo en línea. Fundamental a este respecto es la interconexión en la cual se funda internet, producto de la cual la información generada en un ordenador es procesada por una serie de servidores y redes, de manera previa a alcanzar su destino.

En este contexto se habla de los sniffers, programas que se utilizan para interceptar información en la red y de los rootkits, que permiten borrar las huellas dejadas después de una intrusión, así como del superzapping, líneas especie de llave maestra cibernética y del "pinchado" de líneas.[46]

Esto se conjuga con el hecho de que el desarrollo tecnológico una nueva forma de intercambio a dicha información, sino que además la constante evolución de las herramientas utilizadas para su interceptación, las cuales son cada vez más sofisticadas y eficaces en su propósito.

[44]Barinas, Désirée op. cit. p. 15.
[45] La Rue, Frank ibid. p 5.
[46] La Rue. op. cit p.21.

En cuanto a los métodos de vigilancia masiva efectivamente utilizados, estos son poco conocidos, lo cual es una consecuencia directa del secretismo que rodea a esta actividad. Sin embargo, con las revelaciones de Edward Snowden quedaron al descubierto algunos programas utilizados por las agencias de inteligencia.[47] Así. Con el nombre de PRISM se conoce al programa de vigilancia a cargo de la NSA, bajo el amparo de la legislación norteamericana, específicamente FISA. Su objetivo era descargar datos de internet y voz de IP directamente de nueve de los mayores proveedores de servicios de internet a nivel nacional, así como datos generados en tiempo real.[48] En particular, este programa se encargaba de recopilar "datos recuperados desde su sistema incluyendo emails, chat (video y voz), fotos de video, datos almacenados, VoIP, transferencia de archivos, video conferencias, notificaciones de actividad de objetivos, detalles de redes sociales en línea, y requerimientos especiales."[49]La extensión del programa es tal, que permite monitorear el audio en tiempo real de aquellas conversaciones realizadas por teléfonos convencionales. En el caso de que la comunicación se desplegará por completo de forma online, el monitoreo permitía acceder tanto al audio, video, chat y archivos transferidos.[50]

UPSTREAM, al igual que PRISM, es un programa desarrollado y utilizado por la agencia de inteligencia estadounidense Nacional Security Agency. Este permitía interceptar y cargar el tráfico doméstico e internacional de telefonía y de tráfico realizado en internet. Esto se logra por medio de mecanismos insertos en las compañías proveedoras de servicios de telecomunicaciones, mientras el proceso de enrutado desde y hacia servidores de todo el mundo se está llevando a cabo.[51] Un rasgo característico de este programa es la vinculación entre la agencia de inteligencia y la compañía de telecomunicaciones de la cual se obtienen los datos, toda vez que esta última era la encargada de realizar el primer filtro respecto de la información recopilada. Esta tarea se realizaba en aplicación de los algoritmos provistos por la NSA, los cuales tenían por objetivo que en desarrollo de la vigilancia, a lo menos se

[47] Para profundizar en la materia consultar entrevista a Edward Snowden en la cual explica el funcionamiento de estos programas <https://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript>
[48] D. Cohen, Elliot. (2014). Technology of oppression: Preserving Freedom and Dignity in Age of Warrantless Mass Surveillance. New York, Palgrave MacMillan, p.19.
[49] D. Cohen, Elliot. ibid. p.20.
[50] Ídem.
[51] Ídem.

interceptara a una persona, de la cual existía una expectativa razonable de poseer información de inteligencia significante, pero se encontraba en el extranjero.[52]

1.3 La vigilancia masiva y otros derechos

1.3.1 Libertad de expresión

La libertad de expresión, como derecho fundamental, es considerado como un pilar fundamental de toda sociedad democrática[53], siendo reconocido tanto a nivel nacional como internacional. Entre aquellos instrumentos internacionales que la recogen se encuentra el Pacto de derechos civiles y políticos, como la Convención Americana de Derechos Humanos.

A nivel nacional, la Constitución Política de la Republica se encarga de reconocer y proteger el derecho a la libertad de expresión, señalando en el artículo 19 n°12 que "La Constitución asegura a todas las personas: […] 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, la que deber ser de quórum calificado."

Se reconoce la libertad de expresión sin condicionamiento o censura previa que puedan coartar su ejercicio.[54] Esta característica ha sido denominada como "preeminencia normativa." Así lo ha señalado el Tribunal Constitucional, al delimitar el núcleo esencial de

[52]Ídem.
[53]Galván, Ezequiel Rodrigo (2016) Libertad de expresión e Internet. [en línea] Disponible en <http://sedici.unlp.edu.ar/bitstream/handle/10915/58287/Documento_completo.pdf-zDFA.pdf?sequence=1&isAllowed=y> [Consultado el 22 de septiembre de 2018] p.46.
[54]Ayala Corao, Carlos M. (2000). El Derecho Humano a la Libertad de Expresión: Limites aceptados y responsabilidades ulteriores. Ius et Praxis [en línea] Disponible en:<http://www.redalyc.org/articulo.oa?id=19760106> [Consultado el 22 de septiembre de 2018]

la libertad de expresión, el cual reconoce que estas "libertades se puedan ejercer sin censura previa, lo que a su vez implica que el ejercicio de tales libertades conlleve una responsabilidad para quienes las ejercen."[55]

En este sentido, el Tribunal Constitucional Federal alemán ha señalado que, en atención al especial contenido de la libertad de expresión, especialmente de su importancia dentro de una democracia liberal, existiría una presunción básica respecto de su ejercicio en toda esfera de desarrollo de la actividad humana.[56] La relación de esta consideración en conjunto con la "preminencia normativa" derivan en la excepcionalidad de su restricción, aun cuando esta se fundamente en consideraciones tales como de seguridad nacional.[57]

Sin embargo, y según el Tribunal Europeo de Derechos Humanos el Estado igualmente se encuentra habilitado para establecer restricciones o sanciones al ejercicio de la libertad de expresión, siempre que esto derive de necesidades urgentes y que estas se constituyan como excepciones legitimas al derecho consagrado.[58] Así, la vigilancia masiva importa una actividad que, cumpliendo determinados requisitos, permite establecer restricciones o mermas en el ejercicio de ella. Estas, sin importar su fundamento, deberán sujetarse a determinados estándares, en específico, la proporcionalidad de su aplicación, así como el respeto a las normas internacionales en materia de libertad de expresión.[59]

Es en cumplimiento de estas exigencias, tal como se ha mencionado, que se debe atender a la "presunción de preminencia" de la libertad de expresión. De su aplicación se deriva que, en caso de duda, conflicto en el juicio de ponderación, deba atenderse a la postura más favorable para la protección y ejercicio de la libertad de expresión.

---

[55]Sentencia del Tribunal Constitucional del 30 de octubre de 1995, rol N°226-95, considerando noveno.
[56]Vidal Prado, Carlos. (2017). La libertad de Expresión en la Jurisprudencia del Tribunal Constitucional Federal Alemán. Estudios Constitucionales Año 15, N ° 2, 2017, pp. 273-300 [en línea] Disponible en:<http://www.redalyc.org/articulo.oa?id=82054982008> [Consultado el 2 de octubre de 2018] p. 292.
[57] Ídem.
[58]Fernández Segado, Francisco (1990) La libertad de expresión en la doctrina del Tribunal Europeo de Derechos Humano. [en línea] Disponible en <http://roderic.uv.es/handle/10550/47836> [Consultado el 20 de abril de 2018] p. 95.
[59]Botero, Catalina Libertad de Expresión e Internet. (2013) Relatoría Especial para la Libertad de Expresión Comisión Interamericana de Derechos Humanos. [en línea] Disponible en <http://pensamientocivil.com.ar/system/files/2014/07/Miscelaneas115.pdf.> (Consultado el 24 de septiembre de 2018) Apéndice 2° p.1.

En consecuencia, de la evolución en el ejercicio de la libertad de expresión por la introducción de las nuevas tecnologías de la información, es que se ha extendido su tutela a cualquier medio o plataforma.[60] En este sentido, la Comisión Interamericana de Derechos Humanos ha expresado que "el artículo 13 se aplica plenamente a las comunicaciones, ideas e informaciones que se difunden y acceden a través de internet."[61] A pesar de esto, si debe atenderse al medio especifico por el cual se ejercita, ya que de acuerdo a las características y particularidades de la plataforma, se determinarán las medidas necesarias para asegurar su correcto ejercicio y resguardo, en caso de vulneración.[62]

En cuanto a su ejercicio, la libertad de expresión, a pesar de ser una garantía reconocida de forma universal, ha sido históricamente asociada a la labor informativa desarrollada por los periodistas, ya sea por medios de comunicación escrita, digital u otros. En este sentido la Corte Interamericana de Derechos Humanos (en adelante CIDH) ha reconocido esta intrínseca relación, al reconocer que "la profesión de periodista implica precisamente buscar, recibir y difundir información. El ejercicio del periodismo, por tanto, requiere que una persona se involucre en actividades que están definidas o incluidas en la libertad de expresión (…). "[63] De igual forma, el Tribunal Europeo de Derechos Humanos se ha manifestado señalando que se deriva del artículo 10 del Convenio Europeo de Derechos Humanos, siendo esta parte integrante de la libertad de comunicación y difusión, así como de la libertad de prensa.[64]

La amenaza que implica la vigilancia masiva para el ejercicio de la libertad de expresión se encuentra estrechamente vinculada a la privacidad, tal como lo ha señalado el Relator Especial de la Organización de las Naciones Unidas: "La injerencia indebida en la

[60] Ídem.
[61] Botero Marino, Catalina. op. cit. p. 70.
[62] Ídem.
[63] García Ramírez, Sergio y Gonza, Alejandra. (2007). Jurisprudencia de la Corte Interamericana de Derechos Humanos. [en línea] Disponible en <http://anaforas.fic.edu.uy/jspui/bitstream/123456789/25380/1/libertad-expresion.pdf.> [Consultado el 20 de septiembre de 2018] p. 24.
[64]Podkowic, Jan. (2015) Vigilancia y privilegio periodístico en la era de las nuevas tecnologías de las telecomunicaciones bajo la Convención de Derechos Humanos y Libertades Fundamentales y la Constitución de la República de Polonia. [en línea] Disponible en <https://dialnet.unirioja.es/servlet/articulo?codigo=5265507> Consultado el 24 de septiembre de 2018. p. 7

intimidad de las personas puede limitar en forma tanto directa como indirecta el libre intercambio y evolución de ideas."[65]

Doctrinariamente se ha reconocido que los métodos de vigilancia masiva, importan dos tipos de violaciones a la libertad de expresión. La primera de estas ha sido denominada como directa, la cual implica que el derecho no puede ejercitarse adecuadamente de manera anónima, como consecuencia de la actividad de vigilancia[66]. El segundo tipo de violación es de carácter indirecta, y supone que tan solo la mera sospecha del desarrollo de la vigilancia produce un efecto inhibitorio tal, que coarta el ejercicio legítimo del derecho.[67]

La afectación directa se manifiesta con la pérdida del secreto propio de la actividad periodística, la cual se encuentra orientado a la protección de la fuente que ha revelado la información. El uso de fuentes confidenciales es común y ampliamente aceptado, considerándose una de las herramientas más útiles para el desarrollo de esta labor, al proveer material que permite dar a conocer a la opinión publica información sobre delitos, irregularidades y otras prácticas, que de otra forma quedaría oculta. [68] El Tribunal Europeo de Derechos Humanos, al pronunciarse al respecto, ha señalado que la reserva y secreto de las fuentes es un derecho integral al derecho a la información. De esto se deriva que, ningún tipo de consideración respecto de estas puede mermar su protección. [69]

Este efecto inhibitorio de la actividad de vigilancia, entendido como afectación indirecta, es consecuencia de la utilización de esta como un método de control social. A pesar de que en cierta extensión el control social es deseable, la conciencia o mera sospecha de la existencia de un monitoreo continuo e invasivo, puede llevar a una persona a alterar su conducta, resultando en una especie de autocensura e inhibición. [70]

---

[65] Podkowic, Jan. ibid. p 7.
[66] Botero Marino, Catalina. op. cit. p. 73.
[67] Ídem.
[68] Podkowic, Jan. op. cit. p. 217.
[69] Tribunal Europeo de Derechos Humanos Caso Tillack v. Belgica. Solicitud 20477/05, del 27 de noviembre de 2007. Apéndice 97. Disponible en < https://hudoc.echr.coe.int/eng#{"fulltext":["tillack"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-83527"]} >
[70] Solove J, Daniel. Understanding Privacy. op. cit. p.108.

La incertidumbre y temor de que terceros adquieran conocimiento de información importante e incluso sensible, puede llevar a no querer exponerla por miedo a las consecuencias o represalias que se puedan generar.

El libre ejercicio de la libertad de expresión, además se imposibilita si se considera el potencial de la vigilancia masiva, para ejercer censura respecto de los medios y de los periodistas en particular. La tecnología que posibilita la vigilancia masiva permite filtrar y por consiguiente realizar un examen constante de la utilización de determinados términos o búsquedas. De esto se deriva que los Estados puedan usar estas tecnologías para detectar el empleo de palabras o frases específicas y censurarlas o reglamentar su uso, o establecer quiénes las usan.[71]

La CIDH ha señalado que la libertad de expresión es una piedra angular en la existencia misma de una sociedad democrática, considerándose como indispensable para la formación de la opinión pública. Su inexistencia o merma deriva en un atentado a los cimientos de un Estado democrático.[72]

1.4 Pugna entre privacidad y seguridad

Seguridad y privacidad son dos valores que pueden encontrarse en pugna, pero el auge de la digitalización de las comunicaciones, el desarrollo tecnológico y la nueva forma en que la vida moderna se desenvuelve, ha requerido repensar la forma en que el tema ha de abordarse, la preminencia que se le otorgará a una u otra, y, en definitiva, la solución que en un Estado democrático deberá alcanzarse.

La cuestión frecuentemente ha sido planteada en términos tales en que la seguridad y la privacidad son presentadas como excluyentes una de la otra. Sin embargo, tal como lo señala Solove, el resolver esta pugna requiere de la determinación de parámetros de control

[71]Podkowic, Jan. op. cit. p 7.
[72] Podkowic, Jan. ibid. p.17.

y responsabilidad, bajo los cuales, las medidas que se desarrollen en el nombre de la seguridad se lleven a cabo.[73]

La seguridad nacional, en su concepción moderna no encuentra una definición pacífica y, por el contrario, se presenta como un término subjetivo, que se vincula a un estado libre de preocupaciones, bajo el cual el sujeto puede sentirse a salvo de cualquier daño que pueda ser infligido por otros[74]. Con el paso del tiempo, se ha incorporado a esta concepción toda política tendiente a la defensa y resguardo de la seguridad en el ámbito interno, incluyendo la protección contra la amenaza terrorista, del crimen organizado, las amenazas ambientales, entre otras.

En el derecho chileno, si bien tampoco posee definición alguna, si encuentra reconocimiento en la Constitución, la cual hace expresa mención de esta en una serie de ocasiones, a saber, como deber del estado, limite a los derechos fundamentales, entre otros.

En concordancia con esta disputa, los diversos instrumentos internacionales, como la misma Constitución chilena, han reconocido la necesidad de limitar la protección del derecho a la privacidad, en post de la protección de otros bienes jurídicos, como la seguridad. Especial importancia adquieren aquellos delitos de mayor connotación social, como el terrorismo en virtud de los cuales, se permiten una serie de transgresiones. las cuales son consideras como necesarias.

Si bien la necesidad de restricción de la privacidad en pos de la seguridad ha sido aceptada, se requiere alcanzar un justo equilibrio, en virtud del cual ninguno sea sacrificado en su totalidad, "La prevención y persecución de los delitos y la lucha contra el terrorismo no puede suponer mermas intolerables en los derechos fundamentales de las personas, si bien la realidad nos muestra como la respuesta de los Estados ante cualquier nueva amenaza a la

[73] Solove, Daniel J. (2007). "I've got nothing to hide and other Misunderstanding of Privacy, [en línea]. Disponible en <https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1159&context=faculty_publications> Consultado el 25 de septiembre. p.771.

[74] Bárcena Cochi, Martha. (2000) La reconceptualización de la seguridad: El Debate Contemporáneo [en línea] Disponible en <https://revistadigital.sre.gob.mx/images/stories/numeros/n59/barcena.pdf> [Consultado el 12 de abril de 2018.] p.12.

seguridad es un recorte a las libertades especialmente de aquellas que garantizan la esfera privada de las personas" [75]

El optar por otorgar preminencia absoluta a la seguridad en desmedro de los derechos fundamentales, implica no desconocer los valores bajos los cuales el Estado moderno se funda, despojando de toda importancia las consideraciones de libertad y dignidad, propias del respeto a los derechos fundamentales.[76]Esto es de especial importancia, toda vez que, las consideraciones en torno a la protección de la seguridad nacional no se contraponen a meras expectativas de la sociedad, sino que por el contrario, a derechos fundamentales que limitan y determinan el actuar del ente estatal.[77]

Al respecto, el Tribunal Europeo de Derechos Humanos, así como el Tribunal de Justicia Derechos Humanos de la Unión Europea, ha establecido criterios en la materia, los cuales si bien reconocen la necesidad de asegurar los medios por los cuales se ha resguardar la seguridad nacional, imponen una serie de restricciones en cuanto a la forma en que estas actividades han de llevarse a cabo. Estos criterios atienden a la necesidad de conciliar el resguardo de los derechos fundamentales, con el desarrollo de políticas de seguridad.

Dos consideraciones esenciales deben efectuarse al realizar un análisis concerniente a las medidas tomadas en nombre de la seguridad nacional; la razonabilidad y su efectividad.

La razonabilidad se determina al sopesar el interés por resguardar la seguridad, con el interés de la población de ejercer de sus libertades civiles, en específico de su privacidad.[78] En definitiva, implica un análisis de proporcionalidad en el caso en concreto.

La efectividad, en cambio, atiende a los resultados mismos de las medidas, en cuanto a si estos pueden ser considerados como óptimos o no. La determinación de este factor es de especial importancia, toda vez que permite determinar la eficacia de las políticas adoptadas. En definitiva, la preponderancia del interés de seguridad nacional solo puede ser impuesto

[75]Garriga Domínguez, Ana op.cit. p. 52.
[76] Solove J, Daniel, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. op. cit. p. 764.
[77] Barinas, Déssirée op. cit. p.54.
[78] Solove, Daniel J. (2008). Data mining and the Security-Liberty debate. [en línea] Disponible en < https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=5659&context=uclrev> Consultado el 25 de septiembre de 2018. p.348.

en la medida en que efectivamente por medio de una demostración empírica, este haya resultado en un incremento de la seguridad.[79]

El control judicial a priori y posteriori, como una solución al conflicto, ha sido una extensamente reconocida. Las ventajas de éste radicarían en que permite realizar un examen exhaustivo y en concreto respecto las intromisiones y riesgos a los cuales la población, y los sujetos en particular, se encuentran expuestos con la vigilancia. A pesar de esto, se ha señalado que dicho control atentaría contra la labor legislativa realizada, al atender a distintos factores para determinar la procedencia y extensión de las medidas de vigilancia.[80]

Una de las soluciones propuestas para resolver esta dicotomía, se encarna en el popularizado "el que nada hace, nada teme" o "If you've got nothing to hide, you've got nothing to fear", de acuerdo al cual, si las personas no han hecho nada malo (en el sentido de la comisión de un delito), nada deben temer del ejercicio de actividades de vigilancia continuas por parte del Estado.

Esta solución presenta un problema estructural al alterar la forma en la cual la privacidad se concibe, ya que tal como lo ha señalado Solove, bajo el argumento de "nothing to hide", subyace la suposición de que la privacidad tiene por objeto el ocultar información o cosas.[81] Es más, reduce el derecho a la privacidad a una concepción simplista, la cual la entiende solamente como una forma de secreto, de suerte que por medio de esta se pretende esconder un aspecto negativo de la vida de alguien, generalmente relacionado con una actividad ilegal.[82] Esto es contrario al desarrollo doctrinal y jurisprudencial contemporáneo realizado en torno a la privacidad, el que ya no tan solo la concibe como una forma de secreto, sino que además como una forma de control, retiro, la posibilidad de aislarse y ejercer poder respecto de uno mismo.[83] El reconocimiento de la privacidad como derecho fundamental, en ningún punto de su desarrollo o evolución ha pretendido el ocultamiento de información

[79] Ídem.
[80] Solove, Daniel j. Data mining and the Security-Liberty debate. ibid. p.346
[81] Solove, Daniel J. (2011). Nothing to hide: The false Tradeoff Between Privacy and Security. Yale University Press p.26.
[82] Solove, Daniel J, ibid.p.26.
[83] Para profundizar en las distintas concepciones de la privacidad consultar Solove "Conceptualizing Privacy".

referente a actividades ilegales, por el contrario, incluso en su uso más generalizado y común, solo es reclamada para el resguardo de cuestiones completamente legales.

Lo que esconde el argumento en cuestión es un juicio previo de ponderación entre seguridad y privacidad, el cual ha sido resuelto en favor del primero de estos, sin a lo menos plantear la existencia de una tensión entre ambos. Consecuencialmente, se disminuye el valor inherente de la privacidad, al asumir que la vigilancia y control de actividades legales no tendrán un efecto negativo en los sujetos afectados, en comparación a los supuestos beneficios reportados.[84]

La adopción de un enfoque en esta materia rebasa las pretensiones de un análisis constitucional y adquiere significancia en el derecho penal. Un sacrificio total, o de mayor entidad de la privacidad, en comparación de la seguridad, es una expresión del cambio desde una política de tutela preventiva, garantista, a un modelo penal de "seguridad ciudadana", en el que la incorporación de nuevas tecnologías que permiten la vigilancia continua y oculta es la norma.[85]

En definitiva, la adopción de una u otra postura solo deja de manifiesto la dificultad de la cuestión tratada, ya que sin importar la decisión que se adopte, está usualmente resultará en una que no promueva con máxima eficiencia los derechos en juego.

1.5 Derecho a la privacidad en el derecho chileno

La garantía constitucional de la privacidad se encuentra consagrada en el artículo 19 n°4 de la Constitución, la cual dispone: "La Constitución garantiza a todas las personas: 4° El respeto y protección a la vida privada y a la honra de la persona y su familia y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará

[84] Solove, Daniel J, Nothing to hide: The false Tradeoff Between Privacy and Security op. cit. p.29.
[85]Barinas, Déssirée op. cit. p.56.

en la forma y condiciones que determine la ley." A su vez, diversos tratados internacionales ratificados y vigentes en Chile reconocen el derecho a la privacidad.[86]

Conceptualizar este derecho, en conformidad a lo establecido por la Carta Fundamental, ha sido una tarea abordada tanto por la jurisprudencia constitucional como por la doctrina. El Tribunal Constitucional (en adelante TC) ha entendido la privacidad como "la situación de una persona, en virtud de la cual se encuentra libre de intromisiones de agentes externos y ajenos a su interioridad física o psicológica y las relaciones que mantiene o tuvo con otros."[87] En este mismo sentido ha señalado que comprende un ámbito de no intromisión reservado de la vida personal[88], así como, el conjunto de los asuntos, conductas, documentos, comunicaciones, imágenes o recintos que el titular del bien jurídico protegido no desea que sean conocidos por terceros sin su consentimiento previo.[89] Queda de manifiesto en esta definición la íntima vinculación existente entre la privacidad y otros derechos fundamentales como el secreto o inviolabilidad de las comunicaciones, los cuales han sido considerados como derivaciones o manifestaciones del derecho a la privacidad en determinados ámbitos del desarrollo de la vida de las personas. Asimismo la Comisión de Estudio para una Nueva Constitución Política de la República comprendió el derecho a la privacidad, ya desde su relación con los incipientes avances tecnológicos, señalando que existía una necesidad imperiosa de consagrarla en el nuevo texto fundamental toda vez que "que dado el avance de la ciencia electrónica y de otros medios, es posible interferir en la vida particular de cualquier individuo, obteniendo toda clase de información sobre su vida privada." [90]

La doctrina nacional se ha manifestado en concordancia a lo ya expresado, y Hernán Corral la define como "la posición de una persona (o entidad colectiva personal) en virtud de la cual se encuentra libre de intromisiones o difusiones cognoscitivas de hechos que

[86] Así lo reconoce el Pacto de Derechos Civiles y Políticos, Convención Interamericana de Derechos Humanos y otros tratados sectoriales como La Declaración Universal de los Derechos del Niño.
[87] Navarro Beltrán, Enrique y Carmona Santander, Carmona. (2005) Recopilación de Jurisprudencia del Tribunal Constitucional (19812005). Cuadernos del Tribunal Constitucional. N° 59. p.190.
[88] Sentencia Tribunal Constitucional de 12 de julio de 2012, rol N°1894-2011, considerando vigésimo primero.
[89] Sentencia Tribunal Constitucional de 5 de junio de 2012, rol N°1990-11, considerando vigésimo tercero.
[90]Comisión de Estudio de la Nueva Constitución, Acta Oficial. Segunda parte de la sesión 83° el jueves 31 de octubre de 1974, p.385.

pertenecen a su interioridad corporal y psicológica o a las relaciones que ella mantiene o ha mantenido con otros, por parte de agentes externos que, sobre la base de una valoración media razonable, son ajenos al contenido y finalidad de dicha interioridad o relaciones."[91]

Estas definiciones, si bien diversas, comparten una característica fundamental aceptada por el TC, esto es, la necesidad de reconocer y resguardar el núcleo esencial del derecho a la privacidad compuesto por la dignidad y libertad de las personas frente a posibles intromisiones arbitrarias e ilegales de cualquier tipo.[92] En este orden de ideas, el fundamento bajo el cual se ha construido la protección de la privacidad a nivel nacional es "la necesidad de garantizar un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario para mantener una mínima calidad de vida humana, que no puede ceder ante la prevalencia de otros derechos."[93]

Este ámbito de resguardo reconocido y tutelado en el derecho nacional, expresión del sentido negativo de la privacidad, debe ser reconducido a la relación intrínseca con la protección a la dignidad humana, así como el resguardo de la autodeterminación individual.

Esta relación encuentra su origen en la misma base del sistema constitucional chileno, el cual dispone en el artículo 1° de la CPR que "Las personas nacen en libres e iguales en dignidad y derechos." La dignidad humana sobre la cual se fundan las garantías fundamentales, y en específico el derecho a la privacidad, es entendida como aquella cualidad que detentan los seres humanos por la sola razón de ser tal, que los hace acreedores de un trato respetuoso, toda vez que ella se constituye como fuente de derechos y garantías fundamentales destinadas a obtener su resguardo.[94]

De igual forma el TC se ha pronunciado señalando que, "el respeto y protección de la dignidad y de los derechos a la privacidad de la vida y de las comunicaciones, son base esencial del desarrollo libre de la personalidad de cada sujeto, así como de su manifestación

[91]Corral Talciani, Hernán. (2000) Configuración Jurídica del derecho a la privacidad, Revista Chilena de Derecho, Vol. 27 N°2. p. 17.
[92]Rayman Labrín, Danny op. cit. p.195.
[93]Navarro Beltrán, Carmona Santander, op. cit. p. 196.
[94]Sentencia Tribunal Constitucional del 28 de octubre de 2003, rol N° 389, considerando décimo séptimo.

en la comunidad a través de los grupos intermedios autónomos con que se estructura la sociedad."[95]

Así la dignidad humana se posiciona como el principio matriz que informa al sistema constitucional chileno, del cual se deriva que todo ser humano está dotado de esta cualidad, sin distinción o exclusión de cualquier tipo. Es esta matriz la que se constituye como fuente de los derechos fundamentales asegurados en el artículo 19 de la Carta Fundamental.[96]

En cuanto a la autodeterminación que emana de la dignidad humana, esta se manifiesta como la necesidad de autoafirmar al sujeto como digno los derechos y garantías necesarios para su desarrollo individual.[97] La existencia y protección de una esfera privada de desarrollo humano, es indispensable al permitir desarrollo de la autodeterminación del individuo, en cuanto esta solo esta se puede producir en un espacio exclusivo gobernado por cada individuo.[98]

Tal como se ha señalado, el derecho a la privacidad ha sido consagrado e interpretado en el derecho nacional desde una concepción negativa, entendiéndose como una forma de reserva de determinada información del conocimiento de terceros, excluyendo a estos de aquellos aspectos de su existencia que considera íntimos o reservados.

Este sentido negativo atiende a la primitiva distinción entre la dimensión negativa y positiva del derecho a la privacidad, la cual permite comprender este derecho desde un doble enfoque destinado a construir una visión dinámica de este, centrado en la forma en que el sujeto hace ejercicio de él.

En cuanto al aspecto negativo, este permite al individuo encerrarse en sí mismo, excluyendo del conocimiento ajeno aquellos hechos o circunstancias personales que sólo develará si así lo consiente.[99] Esta concepción, si bien recoge parte fundamental del contenido del derecho a la privacidad, es insuficiente en atención a las exigencias del

[95]Sentencia Tribunal Constitucional del 10 de octubre de 2003, rol N° 389-2003, considerando vigésimo primero.
[96] Sentencia Tribunal Constitucional de 20 de abril de 2004, rol N°1273, considerando cuadragésimo segundo.
[97] Ídem.
[98] Sentencia Tribunal Constitucional de 5 de junio de 2012, rol N°1990-11, considerando trigésimo segundo.
[99] Banda Vergara, Alfonso. (2000) Manejo de Datos Personales un Límite al Derecho a la Vida Privada Revista de Derecho (Valdivia), vol.11, p.55-70. p.63

análisis en cuestión. Desconoce la necesidad de control que los sujetos poseen y exigen respecto de su información o datos, centrando su poder respecto de estos en la sola posibilidad de abstracción de la sociedad que este pueda alcanzar. Resta significancia a toda forma de gobierno que el titular de los datos podría tener.

El aspecto positivo, en cambio, entendido como la facultad de la cual estarían dotadas las personas para excluir de la indagación de sus datos e información personal a terceros[100], permite establecer un claro alcance al derecho en comento. Tal como lo ha señalado Enrique Barros, la privacidad considerada dentro de su esfera positiva, se expresa como el poder para excluir a las personas no autorizadas del conocimiento de hechos que quedan bajo el control exclusivo de cada cual. En efecto, se constituye como una forma de control de la cual es titular el sujeto que origina la información, lo que en definitiva tiene por consecuencia el impedir que terceros se introduzcan en ámbitos protegidos por este ámbito de privacidad.[101] Esta concepción del derecho a la privacidad, desde una faz positiva, permite al titular del derecho la facultad de controlar los datos e información relativos a su persona.[102]A mayor abundamiento, este aspecto positivo alcanza a toda información o dato que las personas estimen como reservado, limitando la forma en que estos han de ser indagados y recopilados.

La privacidad, en este entendido, se manifiesta como el ejercicio del control que tiene la persona sobre el flujo de información existente sobre sí misma, y respecto de las acciones ilegitimas o ilegales que puedan efectuarse con el objeto de obtener información, sin que medie autorización alguna.

Esta forma de comprender el derecho a la privacidad es denominada como la moderna concepción dinámica de la privacidad, la cual encuentra en su núcleo la prerrogativa del sujeto de disponer de su información, permitiendo su defensa ante agentes externos. Una manifestación de esta faz positiva se encuentra en la Ley 19.628 sobre Protección a la Vida Privada, la que contempla en su Título II la posibilidad de que el titular de los datos

[100] Banda Vergara, Alfonso. ibid. p 58
[101] Barros Bourie, Enrique. (1998) Honra, privacidad e información: un crucial conflicto de bienes jurídicos Revista de Derecho Universidad Católica del Norte, N°5, pp. 45-58. p. 46.
[102] Banda Vergara, Alfonso. op. cit. p.59.

personales exija su eliminación o modificación, concurriendo determinados supuestos descritos en la ley.

Si bien dicha normativa es insuficiente, toda vez que restringe el control de la vasta información existente respecto de un sujeto a una pequeña porción conformada por los datos personales, sirve como base para construir un reconocimiento más amplio que contemple información que exceda y no se encuentre de forma exclusiva en base de datos.

En definitiva, la normativa nacional discurre sobre la base de la protección de la privacidad desde una perspectiva negativa, la cual solamente se limita a reconocer y amparar la prerrogativa de los sujetos de mantener determinada información en secreto, reservada del conocimiento público. Esto es insuficiente, toda vez que el dinamismo propio de la era tecnológica exige el reconocimiento del dominio particular sobre los datos originados por uno mismo.

1.6 Limitación al derecho a la privacidad en el derecho chileno

Las circunstancias bajo las cuales se ha permitido limitar, parcial o totalmente, el ejercicio del derecho a la privacidad ha sido latamente tratados por el Tribunal Constitucional. A este respecto se han establecido una serie de criterios, los cuales, llevados al caso en concreto, posibilitan la determinación de la validez y concordancia de una actividad con el derecho imperante.

Estos criterios han sido reiterados en múltiples ocasiones, sin que en ninguna de estas se trate o aluda a una actividad equivalente o similar a la vigilancia masiva. Sin embargo, estos parámetros permiten construir el estándar que esta actividad debe alcanzar a nivel nacional.

Se ha dispuesto al respecto un deber general sobre los órganos del Estado, el cual se manifiesta en el imperativo de no llevar a cabo acciones u omisiones, que envuelvan una transgresión o desconocimiento del derecho a la privacidad. Este deber es descrito como

uno de carácter omisivo o pasivo[103], el cual se complementa con un deber de amparo o cautela en post de impedir posibles vulneraciones.

En cuanto a las posibles transgresiones se ha señalado que estas puede provenir de dos vías, a saber, por medio de la intromisión a la esfera privada, así como por la divulgación de información amparada por este ámbito de reserva.[104] En cuanto a la divulgación de información, esta se relaciona con el previamente tratado aspecto positivo de la privacidad, en virtud del cual el sujeto, entendido como titular del derecho en comento, posee control absoluto respecto de la exposición o utilización los datos de su pertenencia.

Ahora, la vulneración que importa a este análisis, esto es, las intromisiones ilegitimas, estas se producen cuando esta zona de retiro y exclusión de terceros es intervenida, ya sea por el Estado o privados, sin autorización legal o de la persona afectada. En este sentido, y en reconocimiento de una facultad de control respecto de los datos e información concernientes a sí mismo, es que se ha establecido como exigencia primordial para la intervención al derecho a la privacidad, el consentimiento del sujeto afectado. Esto importa, de acuerdo a lo dispuesto por el TC, la existencia de un consentimiento espontáneo, el cual sería una expresión del gobierno que las personas poseen respecto de sus propios datos, solamente pudiendo ser suplido dicho consentimiento por la voluntad soberana expresada en la ley.[105]

El análisis en cuestión requiere efectuar un test especifico, el cual examina la normativa bajo los siguientes parámetros; la existencia de habilitaciones restrictas, la existencia de pautas objetivas y sujetas a control que regulen la materia, que las restricciones impuestas sólo afecten al derecho en forma precisa y determinada, que la víctima no padezca detrimentos excesivos de la aplicación de las restricciones, y que estas restricciones tengan por único objetivo el coadyuvar a cumplir objetivos del legislador.

En el mismo sentido, se ha señalado que el acceso a las comunicaciones privadas solo puede tener lugar en aquellos casos en que el legislador lo estime como indispensable para

[103]Sentencia Tribunal Constitucional rol N° 1990-11. ibid. Considerando 32.
[104] Banda Vergara, Alfonso op. cit. p.51.
[105] Tribunal Constitucional de 12 de Julio de 2011, rol N° 1894-2011, considerando vigésimo primero.

una finalidad de relevancia mayor; cuando sea necesario porque no hay otra alternativa disponible y lícita; bajo premisas estrictas; con una mínima intervención y nunca de manera constante y continua, sino que de forma limitada en el tiempo y siempre de modo específico, señalándose situaciones, personas, hechos. [106]Ante la falta de normativa nacional que regule la materia, y que por consiguiente pueda ser contrastada con tales requisitos, se procederá a exponer la forma en que han sido desarrollados por nuestro TC estos requisitos.

La habilitación restricta como requisito impone la exigencia de analizar a la luz de las facultades otorgadas, la limitación del órgano en su actuar, de forma tal que su actuación debe reducirse estrictamente "al ámbito estricto y acotado en que podría hallar justificación."[107] Entendida así, la habilitación legal otorgada con el propósito de vulnerar derechos fundamentales debe conferir para su validez determinadas pautas objetiva y controlables, las cuales además permitan establecer mecanismos de control en orden de asegurar su cumplimiento.[108]

Uno de los puntos de mayor relevancia es la problemática que se produce en relación al periodo de tiempo durante el cual se desarrolla la vigilancia masiva, así como la población afectada por esta. De la esencia de la actividad es su prolongación indefinida en el tiempo, sin que exista certeza por parte del sujeto del tiempo por el cual el monitoreo ha de extenderse, o incluso si este está siendo llevado a cabo. Esta falta de determinación de su extensión es contraria a las exigencias impuestas a nivel constitucional, las cuales en un esfuerzo por proteger y respetar la esencia misma de los derechos fundamentales, requiere de la determinación en este aspecto. Esta prolongación indefinida conlleva además la imposibilidad de que una afectación de las características de la vigilancia masiva puede considerarse como "mínima", ya que sus efectos se presentan como una onda expansiva, la cual irradia a todos los sujetos que han interactuado con aquel que ha visto sus comunicaciones intervenidas.

[106] Sentencia Tribunal Constitucional de 31de enero de 2013, rol N°2246-2014, considerando quincuagésimo sexto.
[107] Sentencia Tribunal Constitucional de 28 de octubre de 2013, rol N° 389-2013, considerando vigésimo quinto.
[108] Ídem.

Esta mínima intervención, además, en atención la masividad de la actividad en cuanto a los sujetos afectados por esta, así como a la extensión indefinida de la información recabada en consideración a la tecnología ocupada para este propósito, de forma alguna es respetada, toda vez que de la exposición de estas características se hace obvio que la intervención que en la práctica se provoca es vasta e incalculable, contrariando plenamente el test en cuestión, sin que existan pautas que determinen en definitiva que sujetos en específico deben ser intervenidos. Una intervención mínima y acotada a sujetos determinados, es la única forma de que dicho criterio podría ser alcanzado.

De ahí que el TC haya rechazado, y considerado inconstitucionales, habilitaciones irrestrictas o sin parámetros objetivos y precisos, facultades absolutamente discrecionales, potestades que no sean estrictamente indispensables, para el desarrollo de actividades de estas características.[109]

Al referirse las pautas objetivas que han de regir en la materia, el TC ha señalado que no se produce el cumplimiento de este requisito en aquellos casos en que se otorgan facultades irrestrictas o indeterminadas, sin que exista limitación alguna que constriña la competencia entregada por la ley a un ámbito estricto y acotado.[110] Este requisito se encuentra directamente relacionado con las exigencias que una ley debe cumplir al imponer restricciones al ejercicio de un derecho fundamental. Esta debe establecer claramente las facultades que otorga, estableciendo un límite al ejercicio de estas.

La determinación de la concurrencia del detrimento excesivo es un requisito que ha de ser valorado al realizar un análisis exhaustivo de la normativa en cuestión. A modo ejemplar, el TC al pronunciarse respecto de la toma de muestra biológicas para la creación del Sistema Nacional de Registros de ADN, determinó que el derecho a la privacidad de los sujetos sometidos a la extracción de su huella biológica no sufría un detrimento excesivo. En específico, al ser considerado este registro como una medida indispensable para la identificación y esclarecimiento de delitos, este cumplía con los requisitos previamente

[109] Ídem.
[110] Ídem.

analizados, lo que derivaba en que el núcleo del derecho a la privacidad se resguardaba y permanecía incólume a injerencias arbitrarias.[111]

Por consiguiente, la determinación del detrimento excesivo responde a dos factores, siendo el primero el análisis de la legislación bajo los estándares impuestos por los requisitos previamente señalados, y en segundo lugar, del respeto del núcleo esencial del derecho a la privacidad. La determinación de ambos requisitos solo puede ser analizados a la luz de una normativa específica.

En adición a estos criterios, el análisis que debe efectuarse respecto de la validez de las medidas intrusivas efectuadas en desmedro del derecho a la privacidad, debe contemplar a el respeto del núcleo esencial de este. Esta consideración importa que "las limitaciones que el legislador imponga al derecho a la vida privada no pueden afectar en su esencia el contenido sustancial de ese derecho, como tampoco imponerle condiciones o requisitos que impidan su libre ejercicio ni privarlo de la debida tutela jurídica."[112]

La determinación de este núcleo esencial no es una cuestión que haya sido especialmente tratada por la doctrina o jurisprudencia nacional, y por esto que a pesar de existir ciertas aproximaciones en el tema, estas son insuficientes para el análisis en cuestión.

La doctrina ha entendido en aquel "ámbito reservado del individuo que no desea ser develado al conocimiento y acción de los demás, el cual aparece como necesario para mantener un mínimo de calidad de vida humana."[113] Esta definición, a pesar de otorgar un acercamiento a lo que compone dicho núcleo, no otorga mayor claridad al respecto, ya que su vaguedad e imprecisión al remitirse a este "ámbito reservado" solo logra reconducir la cuestión a lo que se entenderá protegido por la privacidad.

[111]Sentencia Tribunal Constitucional de 8 de abril de 2010, rol N° 1365-09-INA, considerando trigésimo séptimo.
[112]Sentencia Tribunal Constitucional de 28 de octubre de 2010, rol N ° 389-03, considerando vigésimo segundo.
[113]Nogueira Alcalá, Humberto. (1998). El Derecho a la Privacidad y a la Intimidad en el Ordenamiento Jurídico Chileno. [en línea] Ius et Praxis. Disponible en <http://www.redalyc.org/articulo.oa?id=19740206> [Consultado el 29 de julio de 2018] p.68.

La determinación de este núcleo requiere del análisis jurisprudencial internacional, en específico, la establecida por el TJUE, el cual, posibilita comprender el alcance de la vigilancia masiva, así como la extensión de sus límites.

Este tribunal, al determinar el núcleo o contenido esencial de la privacidad, estableció que este se encontraba determinado por la posibilidad de conocer el contenido de las comunicaciones interceptadas.[114] De esto se deriva la necesidad de distinguir en el caso exclusivo de las comunicaciones, entre su contenido mismo y los metadatos que la componen.[115] Enseguida, el solo acceso al contenido atentaría con el derecho a la privacidad, no importando el proceso de interceptación mismo por medio de la cual se permite adquirir los metadatos de la población afectada.[116]

En el mismo sentido, el análisis se extiende a la conservación de datos, excluyendo a esta de la protección del núcleo esencial. El razonamiento del TJUE discurre en la normativa comunitaria de la materia, la cual impone a los estados miembros de la UE la obligación de establecer medidas técnicas y organizativas, tendientes a la protección de los datos recolectados.[117] A criterio del tribunal dicha protección sería suficiente para velar por el respeto de la vida privada.

Recientemente el TJUE ha establecido que, "en particular, se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada (…)"[118] En este entendido, el tribunal abandona las consideraciones relativas la diferenciación de los elementos de la comunicación

[114]Tribunal de Justicia de la Unión Europea, caso Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros C-293/12, de 8 de abril de 2014. Apéndice 39. Disponible en < http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=2332690 >

[115]Para una aproximación a lo que son los metadatos visitar <https://www.derechosdigitales.org/wp-content/uploads/no-pirawebs-022.jpg>

[116]Tribunal de Justicia de la Unión Europea, caso Maximillian Schrems y Data Protection Commissioner v. Facebook Ireland Limitada. C-498/16, 6 de octubre de 2015. Apéndice. 40. Disponible en < http://curia.europa.eu/juris/document/document.jsf?text=&docid=198764&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=2332690 >

[117] Tribunal de Justicia de la Unión Europea. Schrems y Data Protection Commissiones v. Facebook Ireland Limitada op. cit. Apéndice 52.

[118]Tribunal de Justicia de la Unión Europea ibid. apéndice 94.

interceptada, estableciendo como criterio determinante para el establecimiento del núcleo esencial, la existencia del solo acceso a las comunicaciones o datos privados. Este vuelco jurisprudencial, si bien permite evidenciar la complejidad que existe hasta hoy en la determinación de los límites de la actividad de vigilancia masiva, evidencia de igual manera la evolución en la ponderación realizada entre privacidad y seguridad.

El límite establecido por la primera de las sentencias, al distinguir entre los metadatos de la comunicación y su contenido mismo, igualmente permite conocer determinada información de la persona, la cual, no es del todo irrelevante. Debe considerarse que los metadatos permiten el acceso a los datos personales de los participantes de la comunicación, así como el lugar, fecha y hora de su desarrollo, es más, en relación con la navegación web, proporciona los datos concernientes a los sitios visitados y otros relacionados.[119] La consideración global de dicha información permite procesos que previamente han sido descritos, al analizar el tratamiento de la información, en específico la agregación de datos. En específico, la agregación de datos al habilitar la contrastación y unión de distinta información considerada irrelevante de manera independiente, pero que al ser "agregada", adquiere un valor sustancialmente mayor, permite aseverar que, al igual que el contenido mismo de la comunicación, los metadatos otorgan acceso a información igual de relevante e intrusiva para con el derecho a la privacidad.

Pues bien, al perder relevancia la distinción relativa a la importancia de la información que ambos elementos de la comunicación otorgan, la determinación del núcleo esencial en conformidad con lo establecido por la segunda de las sentencias se presenta como una alternativa comprensiva de los efectos y alcance que poseen los métodos de vigilancia masiva.

La consideración de que el núcleo esencial se encuentra vulnerado en aquellos casos en que el acceso a las comunicaciones por parte de las autoridades públicas se realiza de forma generalizada, permite deducir dos conclusiones. La primera, determinada por la

[119]Puerto, María Isabel y Sferrazza-Taibi, Pietro. (2018) La sentencia Schrems del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional. Revista Derecho Estado n.40 [en línea]. Disponible en < http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S0122-98932018000100209&lng=en&nrm=iso > [Consultado el 25 de noviembre de 2018] p. 227.

comunicación misma, es que la sola intervención a esta constituirá una transgresión a la privacidad, sin que importe las herramientas que se han utilizado para concretar dicha interceptación o el alcance de la misma. La segunda, referida al alcance generalizado de la vigilancia, permite aseverar que si bien se reconoce la necesidad en determinados contextos de una intervención a gran escala de las comunicaciones de los ciudadanos, en post del resguardo de la seguridad nacional, la misma debe estar regida por un criterio de "diferenciación, limitación o excepción en función del objetivo perseguido."[120]

1.7 Privacidad, internet y vigilancia masiva

El vertiginoso desarrollo tecnológico de las últimas décadas, el cual provocó la irrupción de internet, ha tenido por consecuencias una creciente preocupación en cuanto si el derecho a la privacidad alcanza a las distintas actividades desplegadas en la plataforma web, o si, por el contrario, en virtud del libre acceso e interconexión que se deriva de este, tiene por defecto la falta de resguardo de la privacidad en la plataforma. Se ha señalado a este respecto que, "este nuevo contexto nos conduce a la revisión del concepto de intimidad y a valorar la ineludible necesidad de adaptarlo a las nuevas características de las sociedades con un alto grado de innovación y desarrollo tecnológico, especialmente en el ámbito de la información y la comunicación".[121]

Primeramente, en cuanto a si el derecho a la privacidad puede extenderse a la plataforma de internet o no, debe señalarse en concordancia con lo señalado por el TC que esta garantía "comprende un ámbito de no intromisión en un aspecto reservado de la vida personal, que cierra el paso a las indagaciones de otros, sean agentes estatales o privados."[122] De esta afirmación se pueden extraer dos conclusiones: en primer lugar, que dicha protección alcanza a aquellas actividades que se desarrollen en internet, toda vez que nos encontramos ante un derecho humano que debe ser respetado en todos los ámbitos en que se despliegan

[120] Tribuna de Justicia de la Unión Europea, Schrems v. Facebook Irelandad. op. cit, apéndice 93.
[121] Martínez de Pisón, José. (2016) Vida Privada sin Intimidad. Una Aproximación a los Efectos de las Intromisiones Tecnológicas en el Ámbito Intimo. [en línea] Disponible en < https://www.researchgate.net/publication/320901364_Vida_privada_sin_intimidad_Una_aproximacion_a_los_efectos_de_las_intromisiones_tecnologicas_en_el_ambito_intimo > [Consultado el 2 de noviembre de 2018]. p. 56.
[122] Sentencia Tribunal Constitucional de 12 de julio de 2012, rol Nº 1894-2011, considerando vigésimo primero.

las actividades que conforman la vida, el cual obviamente evoluciona en conformidad a la realidad en la cual se encuentra inmersa. En segundo lugar, que la referida protección comprende no tan solo agentes privados, sino que es extensible al aparato estatal, lo que deriva directamente en que toda actividad de vigilancia masiva debe estar regulada en la ley, por aplicación directa del principio de legalidad.

Establecida la cuestión precedente, toda vez que nos encontramos con una materia que solamente desde hace pocos años ha cobrado la importancia jurídica que necesita, se hace necesario establecer los límites y extensión que las garantías constitucionales, en especial la privacidad, tienen en internet. El TC ha reconocido que "si bien esta red informática mundial configura un espacio abierto a todos, los sitios visitados en un recorrido, así como los correos electrónicos y la mensajería instantánea allí producidos, revisten carácter confidencial."[123] Este carácter confidencial de los correos electrónicos se encuentra amparado, además, por lo dispuesto en la Ley N° 19.923, la cual tipifica figuras penales relativas a la informática, estableciendo en el artículo 3°: "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."

A mayor abundamiento, este tipo de comunicaciones digitales, en conformidad por lo dispuesto por el TC, se encuentran amparadas por la garantía contenida en el artículo 19 N° 5 de la Constitución, esto es, la inviolabilidad de las comunicaciones privadas. En este sentido el TC se ha pronunciado señalando que la protección que se otorga a las comunicaciones digitales abarca su contenido sin importar si importar si este fue emitido por un canal público o privado.[124] Se garantiza por consiguiente, la protección de la comunicación desde una doble perspectiva, la primera en consideración del derecho a la privacidad, y la segunda en atención a la inviolabilidad de las comunicaciones.

[123]Sentencia Tribunal Constitucional de 7 de enero de 2011, rol N° rol Nº 1894-2011, considerando vigésimo tercero.
[124]Sentencia Tribunal Constitucional de 11 de septiembre de 2012, rol N° 2153-11-INA, considerando trigésimo primero.

En consonancia con lo expresado por el TC, en los casos de plataformas digitales utilizadas con el objeto de transmitir algún tipo de comunicación la protección otorgada por la Constitución alcanza al contenido de esta sin importar si este pertenece o no al ámbito de privacidad del sujeto. Esto quiere decir que, sin importar el canal utilizado (público o privado), la protección constitucional se presenta por el solo hecho de constituirse como una forma de comunicación.[125] En este sentido el TC se ha pronunciado señalando que la "inviolabilidad es una presunción *iuris et de iure* de que lo que se transmite es parte de la privacidad de las personas, por lo que la revelación de ello, independientemente de su contenido, vulnera el derecho de la privacidad."[126]

De esta manera se establece un principio básico el cual determina que sin importar el carácter público de internet, existe una expectativa legitima por parte de sus usuarios de resguardar las comunicaciones y la información que ahí se intercambia, no siendo determinante, para estos efectos, el contexto público el cual puede constituir en ocasiones internet. En cuanto a las plataformas protegidas por el derecho a la privacidad, el correo electrónico ha sido uno de los analizados por el TC, reflexión que presenta determinadas características que lo hacen extensible a otras plataformas de mensajería instantánea así como de almacenamiento y transmisión de información. Los correos electrónicos han sido comprendidos dentro de las llamadas comunicaciones privadas, siendo estos amparados por el derecho de privacidad y el de inviolabilidad de las comunicaciones de las personas que intervienen en el proceso transmisión de la comunicación. Los correos son entendidos como una forma de comunicación, puesto que a través de estos se transmiten mensajes desde un sujeto a un receptor o varios de estos.[127] Esta característica de transmisión de información es propia de todos los servicios de mensajería instantánea, así como de redes sociales y otras plataformas digitales, expuestas a la intervención por medio de la vigilancia masiva.

A diferencia de lo que ocurre con los correos electrónicos u otros servicios de mensajería, los datos originados en las visitas realizadas a sitios web no gozan de dicha protección. Esta

[125] Ídem.
[126] Ídem.
[127] Sentencia Tribunal Constitucional de 31 de enero de 2013, rol N°2246-2012, considerando trigésimo cuarto.

diferencia radica en que no existe transmisión de contenido o comunicación alguna en esta acción, cuestión que, en definitiva, es lo que otorga la protección de la privacidad a estos datos. Al visitar cualquier tipo de sitio o página web, esta acción queda registrada en archivos denominados "/web log_les", lo cual permite fácilmente determinar que objetos fueron requeridos por el sujeto, reconstruir la sesión y realizar en definitiva, un seguimiento completo de la actividad realizada durante la navegación.[128] Si bien son de fácil acceso, la determinación de si esta información se encuentra protegida o no por la garantía constitucional, requiere además de la determinación de si estos pueden ser calificados como sensibles o no, ya que esta consideración permite establecer "el riesgo de que el uso del dato acarree perjuicios a su titular, básicamente por las posibilidades de que terceras personas adopten decisiones arbitrarias a su respecto."[129]

La determinación ultima de si los web data generados en las visitas revisten el carácter de público o privado, recae en la legislación vigente en cada país.[130] En este entendido mientras no exista normativa alguna en la materia, el dueño del sitio web visitado posee control absoluto respecto de los registros que se generen como consecuencia de la navegación del usuario, permitiéndole a este formar un perfil del usuario.[131]

Una segunda característica es la digitalización de la comunicación, la que comprende la transformación de esta en datos o números en base binaria, con el objeto de permitirse su transmisión.[132]

En tercer lugar, el correo electrónico se caracteriza por el hecho de que su transmisión ocurre por medio de la utilización de un canal cerrado, de forma tal que terceros no puedan tener acceso a la información que por éste es transmitida.[133] La transmisión de información por medio de canales cerrados se extiende a todo servicio de mensajería instantánea digital en la actualidad, siendo característico de estos que la comunicación que en esta se realice

[128] D. Velásquez, Juan y Donoso, Lorena. (2009). Web Mining: Análisis sobre la Privacidad del Tratamiento de Datos Originados en la Web. [en línea] Revista Ingeniera de Sistemas. Volumen XXIII, septiembre 2009. Disponible en < http://www.dii.uchile.cl/~ris/RISXXIII/Velasquez5.pdf > [Consultado el 20 de mayo 2018] p. 8.
[129] D. Velásquez, Juan y Donoso, Lorena. ibid. p. 14.
[130] D. Velásquez, Juan y Donoso, Lorena. ibid. p.19.
[131] Ídem.
[132] Ídem.
[133] Ídem.

solo alcance a aquellos destinatarios previamente determinados por los intervinientes de la relación, excluyéndose a todo tercero del contenido de la comunicación. Esta característica alcanza a todo medio digital, incluyendo a aquellas que no están destinadas a la mensajería.

De esta característica se deriva la pretensión de privacidad que se existe respecto de estos medios, toda vez que, se han desarrollado sobre la base de que la información o datos en estos contenidos, solo pueden ser accedidos por su titular o por quienes estos permiten acceso de forma particular. Ejemplificador a este respecto es lo que ocurre con los servicios de telecomunicación de libre recepción, como las concesiones radiales, las cuales de acuerdo con los dispuesto por la ley están destinadas a la recepción libre y directa del público en general.[134] Existe al respecto un conocimiento general de su falta de reserva a un grupo determinado de personas, a la inversa de lo que ocurre con las plataformas de mensajería instantánea, las cuales ni por disposición legal, ni por consideración de sus usuarios son considerados como públicos.

Todas las plataformas digitales mencionadas se caracterizan por su virtualidad, de forma tal que toda interacción que se realice entre los sujetos partes del fenómeno comunicativo toma lugar en el denominado mundo virtual, sin interacción física entre estos.

El TC ha señalado ha incluido además como características de la comunicación digital la instantaneidad, ubicuidad y multidireccionalidad.[135] La instantaneidad hace referencia a la transmisión de alta velocidad en que el mensaje se transmite, lo cual implica que su recepción por el receptor se logre casi en tiempo real.[136]La ubicuidad implica que la comunicación, ya sea este tome la forma de un correo electrónico u otra forma de mensajería electrónica, puede ser recepcionado y abierto por el destinatario en cualquier lugar físico de su elección, siempre que las condiciones técnicas lo permitan.[137] Ilustrativo a este respecto es lo que ha ocurrido con la irrupción de los llamados teléfonos inteligentes o smartphones, los cuales permiten el acceso a correos electrónicos, o mensajes enviados por otra vía digital, en cualquier lugar siempre que el usuario tenga acceso a una conexión a

[134] Artículo 3°, letra a, de la Ley N° 18.168.
[135]Sentencia Tribunal Constitucional de 31 de enero de 2013, Rol N° 2246-2012, considerando trigésimo cuarto.
[136] Sentencia Tribunal Constitucional, Rol N° 2246-2012, ibid. Considerando cuadragésimo cuarto.
[137] Ídem.

internet. Por último, la multidireccionalidad, está determinada por la posibilidad de que en el acto de comunicación participen múltiples sujetos, ya sea en calidad de emisores o receptores, intercambiando estos, constantemente el rol desempeñado.[138]

En este mismo sentido y en relación con la extensión de la privacidad, se debe tener en consideración para su determinación que "la privacidad va más allá de aquello que en internet pueda tener carácter de reservado, ya que también corresponde a la información que nosotros mismos entregamos en internet. De esta forma, importa también el control de la información que se espera sustraer de la observación de ciertas personas, pese a que la hayamos entregado con nuestra autorización."[139]

Se deriva de esto un doble ámbito de protección, el cual se extiende tanto a la información contenida en todos aquellos medios considerados de mensajería, como a aquella que es otorgada de forma voluntaria, sin que este signifique una total divulgación de la información, sino que una entrega parcial a determinadas personas u organismos.

La privacidad en cuento a su extensión, sin embargo, no se agota simplemente con internet, sino que debe comprender, además, cualquier tipo de tecnología en la cual circulen datos e información respecto de la cual, las personas tengan una legítima expectativa de reservarla a su núcleo más íntimo, esto es, la consideren privada. Esta extensión debe comprender, inclusive, todas aquellas herramientas tecnológicas que puedan utilizar los Estados en sus actividades de vigilancia. No comprender los métodos que puedan utilizarse para obtener los datos o información, puede derivar en una protección meramente aparente, que defrauda su propósito al dejar expuesto, aquello que se busca resguardar. De esta forma, la extensión debe abarcar no tan solo las plataformas en los cuales se contiene la información, sino que de igual forma los medios utilizados para acceder a esta, entendiendo por estos todas aquellas plataformas destinadas a la recopilación, almacenamiento y tratamiento de datos.

Es de especial importancia en este apartado establecer que la extensión de la garantía en comento abarca de igual manera a los llamados "datos personales", tal como lo ha expresado el TC, el cual ha declarado que "la protección de la vida privada de las personas

[138] Ídem.
[139] Rayman Labrín, Danny. op. cit. p. 198.

guarda una estrecha relación con la protección de los datos personales, configurando lo que la doctrina, llama derecho a la autodeterminación informativa."[140]

La autodeterminación informativa ha sido conceptualizada como "la posibilidad que tiene el titular de los datos personales de controlar quiénes serán destinatarios de éstos y qué uso les darán, y se ejercita genéricamente a través de los derechos de acceso, rectificación y cancelación."[141]

La inclusión de la autodeterminación informativa al ámbito de protección tiene por efecto que todos aquellos procesos por los cuales se someten a los datos, desde su producción o recopilación, pasando por su utilización o almacenamiento, hasta su eventual divulgación, se encuentran protegidos por la garantía constitucional de privacidad.

En este sentido se puede indicar que delimitada la extensión, la afectación del derecho a la privacidad en la web se produce "cuando existe una intromisión que permite tomar conocimiento de hechos personales reservados, o cuando existe una difusión de esos hechos a personas ajenas o a un público indiscrimado"[142], esto es, cuando aquella información respecto de la cual existe la legitima expectativa de ser reservada, es recolectada, manipulada e incluso divulgada sin previo consentimiento o conocimiento del afectado.

Se ha señalado a este respecto que "este nuevo contexto nos conduce a la revisión del concepto de intimidad y a valorar la ineludible necesidad de adaptarlo a las nuevas características de las sociedades con un alto grado de innovación y desarrollo tecnológico, especialmente en el ámbito de la información y la comunicación."[143]

---

[140] Tribunal Constitucional de 9 de mayo del 2016, rol N° 3016(3026)-16-CPT, voto por acoger, considerando séptimo.

[141] Vazán, Victor. (2005). El Habeas Data y el Derecho de Autodeterminación Informativa en Perspectiva de Derecho Comparado. [en línea] Estudios Constitucionales, vol. 3, núm. 2, 2005, pp. 85-139. Disponible en <https://app.vlex.com/#CL/search/jurisdiction:CL/autodeterminacion+informativa/CL/vid/43011320> [Consultado el 17 de abril del 2018] p.111.

[142] Corral Talciani, Hernán. (2000) Configuración Jurídica del Derecho a la Privacidad II: Concepto y Delimitación. Revista Chilena de Derecho, Vol. 27 N°2 . p.32.

[143] Martínez de Pisón, José. op. cit. p. 56.

CAPITULO II: DERECHO INTERNACIONAL

2.1 Organización de las Naciones Unidas

Como consecuencia de la expansión de las prácticas de vigilancia masiva y el riesgo que estas generan en relación a una serie de derechos fundamentales, el Alto Comisionado de las Naciones Unidas para los Derechos Humanos emitió el año 2014 el informe, "El derecho a la privacidad en la era digital"[144], en el cual se aborda la situación actual de la vigilancia masiva a nivel internacional. El mismo trata los peligros que esta representa en materia de derechos humanos, además de realizar una serie de recomendaciones orientadas a la forma en que han de regular los Estados las actividades de vigilancia masiva.

De forma previa se reconoce que la vigilancia masiva es necesaria en determinados casos, toda vez que, se configura como una medida eficiente y eficaz para los fines perseguidos por las fuerzas policiales o servicios de inteligencia en la persecución de los delitos de mayor gravedad. Sin embargo, como consecuencia de las características que ha adquirido, la vigilancia masiva dado su impacto en la población, debe ser está sometida a un examen que determine su arbitrariedad o ilegalidad. [145]

Se señala en primer lugar, la necesidad de que los Estados de forma inmediata procedan a analizar su legislación en base a el derecho internacional de los derechos humanos.[146] Esto implica determinar cualquier forma de arbitrariedad o ilegalidad no tan solo en consideración al derecho interno, sino que además respecto del derecho internacional.

En cuanto a los criterios impuestos para el examen de la normativa, entiende que la legalidad de las injerencias se encuentra determinada por su consagración expresa, en tanto se considera legal toda aquella injerencia al derecho a la privacidad que encuentre su origen en la ley. Sin embargo, la consagración legal no es suficiente, ya que en aquellos casos en

[144] Alto Comisionado de las Naciones Unidas para los Derechos Humanos, El derecho a la privacidad en la era digital, 2014. [en línea] Disponible en <http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_28_L27.pdf> [Consultado el 1 de abril de 2018]
[145] Ibid. p.6.
[146] Ibid. p.17

que esta es contraria a lo dispuesto por los tratados internacionales, debería considerarse como ilegal.[147]

La arbitrariedad, en cambio, tiene por objeto complementar la determinación de legalidad de una normativa, toda vez que por medio de esta "se pretende garantizar que incluso cualquier injerencia prevista en la ley esté en consonancia con las disposiciones, los propósitos y los objetivos del Pacto y sea, en todo caso, razonable en las circunstancias particulares del caso."[148]

Se requiere de un examen que implique la revisión exhaustiva de la legislación, en cuanto esta permita o no la vigilancia masiva, y la forma y extensión de esta en caso de ser permitida. Se exige además su contrastación con la normativa internacional, para así determinar su conformidad con las exigencias impuestas por los derechos humanos.

Se debe atender al determinar la arbitrariedad de la norma, a lo impuesto por los principios generales de legalidad, proporcionalidad y necesidad. A este respecto se debe garantizar que toda injerencia en el derecho a la privacidad se debe limitar a lo estrictamente necesario para salvaguardar el interés general en una sociedad democrática, lo que se deriva en que toda actividad de vigilancia debe ser proporcional y justa a los objetivos perseguidos.[149] A este respecto, la ley debe cumplir con las exigencias de accesibilidad, claridad y precisión, en cuanto estas permiten que la población pueda leer y comprender el texto legal, de forma tal que sepa en qué circunstancias determinados organismos pueden realizar actividades de vigilancia en su contra, así como los mecanismos que puede utilizar para esto.

---

[147] Ídem.

[148] Naciones Unidas, Asamblea General. Resumen de la mesa redonda del Consejo de Derechos Humanos sobre el derecho a la privacidad en la era digital (2016) A/HRC/2839. [en línea] Disponible en < http://webcache.googleusercontent.com/search?q=cache:DL-7zW4tkdgJ:docstore.ohchr.org/SelfServices/FilesHandler.ashx%3Fenc%3DdtYoAzPhJ4NMy4Lu1TOebIM8c1X4GZjGEGHV9SBM9XSLrkyhn8X9OP5PErl472DFS0WGHKjiDqlMTqWwtmsbg%252B0%252FwzDfM6vlTrrWIR7iAZGazm7af2xJyOwQ13wo5CrT+&cd=1&hl=es&ct=clnk&gl=cl>. [Consultado el 26 de noviembre de 2018] p. 13.

[149] Naciones Unidas, Asamblea General. Resumen de la mesa redonda del Consejo de Derechos Humanos sobre el derecho a la privacidad en la era digital (2016) A/HRC/2839. [en línea] Disponible en < http://webcache.googleusercontent.com/search?q=cache:DL-7zW4tkdgJ:docstore.ohchr.org/SelfServices/FilesHandler.ashx%3Fenc%3DdtYoAzPhJ4NMy4Lu1TOebIM8c1X4GZjGEGHV9SBM9XSLrkyhn8X9OP5PErl472DFS0WGHKjiDqlMTqWwtmsbg%252B0%252FwzDfM6vlTrrWIR7iAZGazm7af2xJyOwQ13wo5CrT+&cd=1&hl=es&ct=clnk&gl=cl>. [Consultado el 26 de noviembre de 2018] p. 13.

La determinación de la arbitrariedad, además, debe contemplar que el objetivo perseguido al efectuar las actividades de vigilancia masiva, pueda ser efectivamente alcanzada por esta, así como que este se constituye como el medio menos gravoso para alcanzar este objetivo, ya que si en atención a los distintos medios que cuenta el aparato estatal, uno diverso conlleva menores este deberá ser el elegido.[150]

En segundo lugar, una vez aplicada la primera medida y en caso de existir deficiencias en la materia, que vulneren o atenten contra los derechos humanos se señala que se " deberían tomar medidas para colmarlas, en particular adoptando un marco legislativo claro, preciso, accesible, integral y no discriminatorio. Deberían tomarse medidas para establecer regímenes y prácticas de supervisión efectiva e independiente, prestando atención al derecho de las víctimas a un recurso efectivo."[151]

Se establece una doble exigencia a los Estados en esta materia. Primeramente, se les impone una obligación en cuanto al contenido de la materia, la que debe respetar las exigencias que impone el respeto de los derechos humanos a nivel internacional, además de disponer de medidas que permitan el acceso a la población a su contenido de forma efectiva. Este acceso debe acompañarse del establecimiento de toda medida tendiente a la comprensión real y efectiva de la legislación.

En segundo lugar, en caso de algún tipo de vulneración de derechos, impone la obligación de hacer efectivo el derecho a un recurso, concebido éste como garantía dentro de un debido proceso.

En cuanto a las injerencias a las cuales se encuentra expuesto el derecho de la privacidad, se establece primeramente como principio general que esta garantía proteger el envío e intercambio voluntario de información personal por medios electrónicos, por parte de los usuarios de la red, sin que pueda entenderse que la utilización de este medio constituye un tipo aceptación por parte de los usuarios para la recolección y tratamiento posterior por quien pueda acceder a esta.[152]

[150]El derecho a la privacidad en la era digital. ibid. p.8.
[151]El derecho a la privacidad en la era digital, ibid. p.18.
[152]El derecho a la privacidad en la era digital. ibid. p. 7.

La falta de información certera y veraz sobre el tratamiento al cual se someten los datos que estos están transmitiendo, impide afirmar que existe algún tipo de consentimiento de su parte, ya que una vez compartidos en internet, los datos han sido recopilados, almacenados y tratados por una serie de servidores, lo que impide que los usuarios tengan control o al menos conocimientos, de quien accede a estos.

A su vez, se establece que las injerencias al derecho de la privacidad se producen en tanto se realicen acciones constitutivas de interceptación o recopilación de datos, así como en los casos en que se procede al manejo del contenido de las comunicaciones privadas.[153] Esta consideración es de especial relevancia, toda vez que el distinguir entre las acciones que permiten la recopilación de la información y el contenido de estas, impide la comprensión de un proceso complejo, compuesto de una serie de etapas o procesos, los cuales solamente considerados en conjunto permiten comprender el alcance que esta actividad tiene. Distinguir entre estas acciones impide reconocer. por ejemplo, la realización de procesos como la agregación, por medio del cual se permite obtener una serie de conclusiones a partir de los metadatos obtenidos por medio de la vigilancia masiva, metadatos que permiten acceder a una serie de conclusiones respecto del sujeto intervenido.[154]

A mayor abundamiento se señala, en relación a las distintas etapas que componen el procesamiento, que la sola interceptación o retención de datos de las comunicaciones, constituye una forma de injerencia de la vida privada, careciendo de importancia alguna si es que efectivamente se consultan, utilizan o se produce el tratamiento de esta información.[155]

2.2 Relatoría de la Libertad de Expresión

[153] Ídem.
[154] Ídem.
[155] Ídem.

La Corte Interamericana de Derechos Humanos, por medio de la Relatoría para la Libertad de Expresión, ha emitido una serie de resoluciones, opiniones y declaraciones conjuntas en relación al desarrollo de la vigilancia masiva.

En sus lineamientos generales se expresa la necesidad de garantizar el resguardo de la seguridad nacional de una forma comprensiva y respetuosa con los derechos humanos,[156] limitando los programas de vigilancia masiva, ya sean operados estos por agentes estatales o privados, requiriendo además del cumplimiento de deberes de transparencia y publicidad, respecto de la información recolectada y tratada.

En este orden de ideas, la Relatoría destaca que la vigilancia masiva, como consecuencia de un desarrollo tecnológico vertiginoso, otorga una serie de herramientas que permiten desarrollar actos particularmente intrusivos que afectan tanto el derecho a la privacidad, como la libertad de expresión. La recolección de datos a gran escala, el rastreo de la actividad en línea, así como de la ubicación en tiempo real de las personas, se constituyen como practica comunes que atentan contra el ejercicio y goce de los derechos previamente referidos.[157]

En cuanto a la necesidad de resguardo de la seguridad nacional ante amenazas como el terrorismo y el crimen organizado, el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, ha señalado que esta puede justificar el uso excepcional de tecnologías de vigilancia masiva de las comunicaciones.[158] Pero el solo pretexto de protección de seguridad nacional no es suficiente, toda vez que: "Este concepto tiene una definición amplia y, por consiguiente, es vulnerable a la manipulación del Estado como medio de justificar medidas dirigidas a grupos vulnerables como defensores de los derechos humanos, periodistas o activistas."[159] Se debe exigir por consiguiente, una delimitación del concepto, el cual debe comprender una regulación exhaustiva en la materia.

---

[157] Relatoría para la Libertad de Expresión Comunicado de Prensa, R 50/15 [en línea] Disponible en <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=990&lID=2> [Consultado el 26 de septiembre de 2018]
[158] Op. Cit. p. 3.
[159] Op. Cit. p. 17.

Es por esto que esgrimir razones de seguridad nacional no implica una habilitación irrestricta para el desarrollo de actividades de vigilancia masiva, sino que, por el contrario, impone la obligación de que esta se desarrolle en un marco normativo adecuado, el cual debe cumplir una serie de requisitos. "La legislación debe estipular que la vigilancia de las comunicaciones por el Estado solo se realice en las situaciones más excepcionales y únicamente con la supervisión de una autoridad judicial independiente. La legislación debe incluir salvaguardias relativas a la naturaleza, el alcance y la duración de las posibles medidas, los motivos que se requieren para disponerlas, las autoridades competentes para autorizarlas y supervisarlas, y el tipo de reparaciones previstas en la legislación nacional."[160]

En este respecto fueron dictados los llamados "Principios globales sobre seguridad nacional y el derecho a la información" o "Principios Tshwane", los cuales, si bien se concentran en la interacción entre la seguridad nacional y el derecho a la información, entrega un guía en cuanto a la determinación de los casos en los cuales la seguridad nacional se encuentre en peligro y al tratamiento de la información. Estos principios establecen una serie de lineamientos en materia de restricción de derechos, los cuales se condicen con los requisitos establecidos a nivel internacional. Aun cuando estos requisitos se establezcan en relación a la libertad de expresión, pueden ser extrapolados y aplicados respecto de otras garantías fundamentales. Pues bien, las limitaciones que se puedan imponer en post de la protección de la seguridad nacional deben estar comprendidas en una ley, ser necesarias para una sociedad democrática, proteger un interés legítimo de seguridad nacional, establecer garantías suficientes en contra de posibles situaciones de abuso y el escrutinio oportuno, pleno, accesible y efectivo por una autoridad supervisora independiente.[161]

[160] Organización para Cooperación y desarrollo Económico, Directrices de la OCDE que regulan la protección de la privacidad y el flujo fronterizo de datos personales, 1981, [en línea] Disponible en <http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf> [Consultado el 1 de abril del 2018] p.22.

[161] Principios Tshwane [en línea] Disponible en < https://www.opensocietyfoundations.org/sites/default/files/tshwane-espanol-10302014%20%281%29.pdf> [Consultado el 20 de septiembre de 2018]

2.3 Directrices de la Unión Europea

Una de las primeras manifestaciones a nivel internacional tendiente a resguardar la privacidad, se presenta por medio de la dictación por parte del Consejo de Europa del Convenio N°108 en el año 1981 "Para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", el cual principalmente se orienta a proteger y garantizar el respeto del derecho a la vida privada en relación al tratamiento automatizado de datos personales, extendiendo dicha protección a agrupaciones, asociaciones, fundaciones, sociedades, compañías o cualquier otro organismo compuesto directa o indirectamente de personas físicas, tengan o no personalidad jurídica. El objetivo primordial de este Convenio es proteger los datos personales del abuso y de la recolección y procesamiento masivo de este, y al mismo tiempo, regular el traspaso fronterizo de datos. [162] La importancia del Convenio radica en que, hasta el día de hoy, es el único instrumento vinculante a nivel internacional en materia de protección de datos personales. [163]

De forma paralela, el año 1981 la Organización para la Cooperación y Desarrollo Económico dictó las "Directrices que regulan la protección de la privacidad y el flujo transfronterizo de datos personales", realizando así un primer acercamiento para el establecimiento de principios que regulen la materia, recalcando la necesidad de "reconciliar los valores fundamentales pero contradictorios como la privacidad y el libre flujo de información"[164], dejando de manifiesto una cuestión que hasta el día de hoy no encuentra solución, esto es, la necesidad de conciliar ambos intereses , a saber el derecho a la privacidad con la obtención y tratamiento de información, que a pesar de ser en principio contradictorios, requieren de una adecuada protección en el marco de un estado respetuoso de los derechos humanos.

Se debe señalar que las referidas normativas solo regulan la utilización, recopilación y tratamiento de datos personales, la cual, no obstante de tener la posibilidad de ser aplicada

[162] Handbook on European Data Protection Law. [en línea] Disponible en <https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdfz > Consultado el 1 de octubre de 2018] p. 16.
[163] Ídem.
[164] Ibid. p.3.

en los casos de vigilancia masiva, al no estar dirigidas específicamente a dicha práctica, desconocen las particularidades que presenta esta actividad en cuanto a la vulneración de derechos fundamentales.

A nivel europeo, se reconoce el derecho en la privacidad tanto en el artículo 8° de la Convención Europea de Derechos Humanos[165] como en el artículo 7° de la Carta de los Derechos Fundamentales de la Unión Europea,[166] la cual, además, consagra como derecho fundamental la protección de los datos personales.

La Unión Europea estima que en ocasiones la privacidad puede ser sometida a un test de ponderación con otros intereses, en específico la seguridad nacional. En estos casos, en que no existe regulación alguna que determine a nivel global la oportunidad, forma e intensidad en que la vigilancia masiva podrá ser utilizada en pos del resguardo de la seguridad nacional, cada país es el encargado de determinarla de acuerdo a su propia normativa en conformidad con el Tratado de Funcionamiento de la Unión Europea[167]. Con el paso del tiempo, han sido dictadas una serie de directivas orientadas a la regulación del tratamiento de datos personales. Una de ellas es la Directiva 95/46/EC del Parlamento Europeo y del Consejo, dictada el 24 de octubre de 1995 la que tiene por propósito fundamental la protección de los datos personales en relación con el procesamiento del que estos pueden ser objeto, y su libre de circulación.[168] Además, fue diseñada con el objetivo de complementar el Convenio 108 de forma tal que los principios concernientes a la privacidad contenidos en este fueran reforzados y expandidos.[169] Una de las cuestiones relevantes introducidas por la Directiva fue la implementación de mecanismos de

[165] Artículo 8 señala: 1. Toda persona tiene derecho al respeto de su vida privada (…).
2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.
[166] Artículo 7 señala que "Toda persona tiene derecho al respeto de su vida privada (…)"
[167] El artículo 4.2 establece las llamadas competencias compartidas, entre las cuales, se encuentra la seguridad. Este tipo de competencia otorgan a los Estados la facultad de ejercerlas autónomamente, siempre que la Unión Europea no haya actuado previamente.
[168]. Handbook of European Data Protection Law. op. cit p.17.
[169] Handbook of European Data Protection Law. ibid. p.18.

supervisión independiente, con el objetivo de mejorar por la protección y tratamiento de datos.[170] Tan relevante ha sido esta normativa que actualmente es vinculante a Estados no miembros de la Unión Europea como Noruega, Liechtenstein e Islandia.[171]

Otras directivas como la 2002/58/EC y la 2006/24/EC han tratado materias previamente reguladas, pero que requerían de una protección más detallada y específica, necesarias para alcanzar un nivel de resguardo y balance entre los distintos derechos e intereses. [172]

En cuanto a la regulación de las comunicaciones electrónicas y la privacidad, la Directiva 2002/58/EC establece los lineamientos y normativa fundamental, permitiendo la utilización del tráfico de datos por el mismo proveedor de servicio (empresa de telecomunicaciones), exclusivamente para la facturación del servicio, así como para cuestiones técnicas relaciones con este. La interceptación de estos datos se encuentra regulada en el artículo 8° del Convenio, debiendo ajustarse a los principios y requerimientos de necesidad, legalidad, entre otros, que posteriormente serán tratados.[173]

2.3 Tribunal Europeo de Derechos Humanos

El Tribunal Europeo de Derechos Humanos (en adelante TEDH), se ha encargado de establecer una serie de parámetros y principios que han de regir en la materia estableciendo las exigencias que debe cumplir la normativa. Si bien se reconoce la prorrogativa de los Estados de establecer con independencia la forma en que ha de combatirse el terrorismo en su legislación interna, se impone la obligación de respetar lo dispuesto por los tratados y convenios internacionales, especialmente, lo dispuesto en el Convenio Europeo de Derechos Humanos.

En concordancia con lo expuesto, el TEDH ha señalado que " la corte estando consciente del peligro que dichas leyes poseen de minar o incluso destruir la democracia con el motivo

[170] Ídem.
[171] Esto fue logrado por medio del Reglamento (CE) N° 1987/2006 del Parlamento Europeo del del Consejo de 20 de diciembre de 2006.
[172] Handbook of European Data Protection Law. ibid. p.19.
[173] Ídem.

de defenderla, afirma que los estados contratantes no podrán, en el nombre de la lucha contra el espionaje y terrorismo, adoptar cualquier medida que ellos juzguen como apropiadas."[174]

En una reciente sentencia, al referirse a lo que se debe entender por vigilancia masiva, ha señalado que esta no se encuentra limitada exclusivamente a la intervención de comunicaciones, extendiéndose a otras formas de "interferencia".[175]

El examen realizado por el TEDH atiende al artículo 8° del Convenio Europeo de Derechos Humanos, el cual asegura el derecho a la vida privada y familiar, además de señalar: *"*No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."

Es en aplicación de este inciso segundo, que los principios de proporcionalidad, legalidad y necesidad se han establecido como aquellos bajo los cuales ha de analizarse esta actividad. La aplicación a la vigilancia masiva, es resultado de la extensión de los requisitos tradicionalmente impuestos a los métodos de vigilancia dirigidos, esto en consideración de que ambos tipos de vigilancia poseen un mismo fundamento, a saber, el desarrollo de un "monitoreo estratégico". Ambos métodos de vigilancia responden a los mismos principios concernientes a la accesibilidad y claridad de reglas que gobiernan la interceptación de comunicaciones.[176]

---

[174] Tribunal Europeo de Derechos Humanos. Caso Klass y otros. v. Alemania, N° 15473/1989. Apéndice 50. Disponible en < https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22\%22CASE%20OF%20KLASS%20AND%20OTHERS%20v.%20GERMANY\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-57510%22]} >

[175] Tribunal Europeo de Derechos Humanos. Caso Big Brother Watch y otros v. El Reino Unido. N° 58170/13 Apéndice 304. Disponible en < https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22big%20brother%20watch%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-186048%22]} >

[176] Tribunal Europeo de Derechos Humanos. Caso Liberty y otros v. Reino Unido. N° 58243/00. Apéndice 63. Disponible en <

2.3.1 El principio de legalidad

Del principio de legalidad se deriva que toda actividad de vigilancia que tenga por efecto la violación o perturbación de la privacidad, deberá estar contenida en la ley, la cual debe cumplir con el requisito de haber sido establecida en forma previa y de manera expresa, taxativa, precisa y clara, tanto en el sentido formal como material.[177] Este reconocimiento legal es un requisito primordial, toda vez que, la intromisión en esferas respecto de las cuales el sujeto posee expectativas legitimas de privacidad, solo puede ser el resultado del proceso legislativo. Este debe ser desarrollado con el objetivo de establecer los antecedentes y condiciones que habilitaran al Estado para intervenir legítimamente las comunicaciones de la población, así como recoger, almacenar y procesar sus datos de comunicación y otro tipo de datos generados en línea, y además someterlas a un monitoreo constante para alcanzar dicho objetivo.[178]

Ejemplar a este respecto es lo dispuesto en el caso Liberty, en el cual se consideró que dicho requisito no era cumplido, ya que a pesar de existir una ley que regulaba la materia, esta había sido sometida con el paso del tiempo a ciertas "adecuaciones", las cuales implicaban cambios significativos en su contenido. [179] La particularidad de estas "adecuaciones" radicaba en que el procedimiento por el cual se efectuaban era uno de carácter administrativo, totalmente diferente al cual se somete una ley. Podría plantearse al respecto si a nivel nacional, por ejemplo, se daría cumplimiento a este requisito en el caso de la dictación de una ley sea complementada por un reglamento.

---

https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22liberty%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-87207%22]} >

[177] Botero Marino, Catalina op cit. p. 74

[178] Klass y otros con Alemania op. cit Apéndice 42.

[179] Respecto a estas adecuaciones, el gobierno británico alegaba que estas solo tenían por objeto adecuar la normativa al desarrollo digital, y no importaban por consiguiente exceder lo dispuesto en la ley.

Las mismas consideraciones son sostenidas por la CIDH, expresando que normas legales vagas o ambiguas que otorgan extensas facultades discrecionales, son contrarias a la protección requerida por el derecho a la privacidad.[180]

La habilitación legal lleva consigo el cumplimiento de una serie de exigencias. En este sentido se requiere que la ley en cuestión cumpla con un determinado estándar material entendido este como la persecución de un fin legítimo. [181]

El mismo atiende a la delimitación del contenido de la ley, y es así como el TEDH ha impuesto como requerimientos mínimos que "la naturaleza de los delitos que darán lugar a la interceptación, la limitación de la duración de la interceptación, el establecimiento del procedimiento que ha de observarse para examinar, utilizar y conservar los datos obtenidos, las precauciones que deben adoptarse cuando los datos son compartidos con terceros, y las circunstancias bajo las cuales los datos pueden y/o deben ser destruidos o eliminados."[182] Igualmente se incluyen como parte de estas exigencias la implementación de mecanismos de supervisión y control, de notificación y de recursos.[183]

Este fin legitimo amparado por la ley, en este caso no otro que la seguridad nacional, [184] pero su sola mención no es suficiente, sino que urge la demostración empírica de que dichas medidas son idóneas y las únicas que en el caso en concreto permiten resguardar la seguridad.

---

[180] Botero Marino, Catalina op. cit., p. 76.

[181] Informe Anual sobre Derechos Humanos en Chile 2017 (en línea). Santiago de Chile, Universidad Diego Portales, 2017. p. 395. Disponible en http://www.derechoshumanos.udp.cl/derechoshumanos/index.php/informe-anual [Consultado el 1 de abril de 2018]

[182] Big brother watch y otros v. Reino Unido. Op. Cit. apéndice 307: "the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which intercepted data may or must be erased or destroyed (see *Huvig*, cited above, § 34; *Valenzuela Contreras*, cited above, § 46; *Weber and Saravia*, cited above, § 95; and *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 76). In *Roman Zakharov* (cited above, § 231) the Court confirmed that the same six minimum requirements also applied in cases where the interception was for reasons of national security; however, in determining whether the impugned legislation was in breach of Article 8, it also had regard to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law (*Roman Zakharov*, cited above, § 238). Traducción propia.

[183] Ídem.

[184] Big Brother Watch y otros v. Reino Unido. ibid, p. 395.

Asimismo, la ley debe permitir que la persona afectada por la vigilancia masiva pueda prever las consecuencias que de su desarrollo se deriven.[185] La previsión de la implementación de la vigilancia no importa el conocimiento por parte del sujeto de que dicha actividad está siendo llevada a cabo en su contra, toda vez que esto contraria a la esencia misma de estas medidas. La ley en cuestión debe permitir al sujeto o población afectada, prever la posible aplicación de esta medida al concurrir determinados supuestos.[186]

El TEDH ha señalado que el requisito de previsibilidad no se cumple en caso de no existir una publicación oficial que informe a la población de la existencia de la ley, no pudiendo ser subsanado este vicio aun cuando, eventualmente la población pueda conocer dicha legislación por otro medio. [187] A esta conclusión arribó el tribunal, al pronunciarse respecto de un caso en el cual el solicitante basaba entre otros argumentos su acción en contra del sistema de vigilancia de su país, en la falta de publicidad de la ley, la cual solo era accesible por medio de la interposición de una acción judicial.

La previsibilidad de la ley, es una cuestión que adquiere especial relevancia en el contexto de un desarrollo tecnológico vertiginoso. Esto conlleva que el riesgo de posibles arbitrariedades aumente exponencialmente, ya que cuando la tecnología utilizada para la vigilancia se vuelve cada vez más sofisticada e impredecible, se requiere de reglas y parámetros claros que determinen claramente el desarrollo de la actividad.[188] En este sentido el TEDH ha señalado que "en cuanto a la discreción legal otorgada al ejecutivo o a un juez de ser expresada en términos de un poder sin limitaciones. Consecuentemente, la ley debe indicar el alcance de tales discreciones entregadas a la autoridad competente y el motivo de este ejercicio con suficiente claridad para entregar la protección individual

[185] Tribunal Europeo de Derechos Humanos, Caso Weber v. Saravia N°54934/00. Apéndice 84. Disponible en < https://hudoc.echr.coe.int/eng#{%22appno%22:[%2254934/00%22],%22itemid%22:[%22001-76586%22]} >

[186] Weber con Saravia. op. cit. Apéndice 93.

[187] Tribunal Europeo de Derechos Humanos. Caso Zhakarov v. Rusia. N° 47436/06. Apéndice 180. Disponible en < https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-159324%22]} >

[188] Tribunal Europeo de Derechos Humanos. Caso Shimovolos v. Rusia. N° 30194/09. Apéndice 68. Disponible en < https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22shimovolos%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-105217%22]}>

adecuada contra interferencias arbitrarias."[189] Para alcanzar dicho objetivo, se requiere además que esta normativa que permite prever el desarrollo de la vigilancia masiva, sea expuesta de forma tal que permite el escrutinio público y conocimiento real por parte de la población.[190]

2.3.2 Principio de necesidad

El principio de necesidad impone, prima facie la obligación de que las medidas adoptadas para llevar a cabo actividades de vigilancia masiva en conformidad a los preceptos legales deben ser aquellas estrictamente necesarias para la obtención de dicho fin.[191] La vigilancia masiva, en ese entendido, debe ser la única herramienta que permita tener acceso a la información necesaria para la protección de la seguridad nacional.

La necesidad, en atención a las actividades de recopilación y tratamiento masivo de datos, se ha entendido que implica que la interferencia a cualquier forma de comunicación debe corresponderse a una necesidad social urgente y la cual en particular debe ser proporcionada al fin legitimo perseguido.[192]

El principio de necesidad puede ser entendido desde dos perspectivas: la primera de estas concibe a este como la última ratio en la búsqueda de la protección de la seguridad nacional, y una segunda, en relación a las exigencias que impone una sociedad democrática.

Del análisis de esta primera perspectiva, se sigue que este principio impone la obligación de que la regulación de la vigilancia masiva, la permita solamente en aquellos casos en que esta sea el único medio existente para la obtención del fin legitimo resguardado por la ley.[193]. En aquellos casos en que la obtención del fin sea posible por diversos medios, se

---

[189] Ídem.
[190]. Tribunal Europeo de Derechos Humanos Liberty y otros v. Reino Unido. op. cit Apéndice 67.
[191] Rayman Labrín, Danny op. cit. p. 224.
[192] Tribunal Europeo de Derechos Humanos. Caso Olsson v. Suecia. N° 74/1991/326/398. Apéndice. 67. Disponible en < https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22olsson%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-57548%22]}>
[193] Rayman Labrín, Danny, op.cit.. p. 224.

debiera optar por aquellos que sean menos lesivos para los derechos fundamentales de las personas. A modo ejemplar, siempre será preferible la interceptación o hackeo, de un solo medio, ya sea una red social o servicio telefónico, que la intervención de todo medio de comunicación y de interacción en la red.

Pues bien, se reconoce a este respecto la facultad de los Estados de determinar la forma que han de adoptar las estrategias de vigilancia a nivel nacional, la cual sin embargo, no implica una discreción ilimitada para subordinar con las medidas de vigilancia secreta a las personas sometidas a su jurisdicción. Esto es consecuencia del reconocimiento de los peligros que conlleva el desarrollo de actividades altamente intrusivas, aun cuando encuentren estas la validación legal.

La necesidad ha sido entendida no tan solo desde los requerimientos que imponen los objetivos de seguridad nacional, sino que se ha integrado a esta, los que se originan como consecuencia del respeto a una sociedad democrática.

El primer pronunciamiento recaído en la materia, ocurrió con la sentencia Klass y otros con Alemania, en la cual el TEDH al pronunciarse respecto a si en el caso en cuestión procedía validar la vigilancia llevada a cabo por la policía estatal como legítima, estableció que los poderes de vigilancia secretan solo eran tolerables en cuanto estos fueran estrictamente necesarios para resguardar las instituciones democráticas.[194] El análisis de esta exigencia debe atender a tres etapas, en las cuales se desarrollan las actividades de vigilancia masiva; la primera comprendida por el momento inicial cuando la vigilancia es ordenada; la segunda, cuando esta toma lugar, y la tercera, una vez que esta ha sido completada.[195]

Respecto a las dos primeras etapas, si bien tal como se ha mencionado previamente, se reconoce y respalda la necesidad del secreto de la actividad, se señala que igualmente estas deberán ser sometidas a algún tipo de control, sin importe que el sujeto o población afectada por la vigilancia no sea parte del proceso. Este control debe proveer por sí mismo garantías adecuadas y equivalentes a las cuales podría optar el individuo si es que este

[194]. Tribunal Europeo de Derechos Humanos, Klass y otros con Alemania, op. cit apéndice 42.
[195] Tribunal Europeo de Derechos Humanos. Big Brother Watch y otros v. Reino Unido. ibid. apéndice 309

tuviera conocimiento de la actividad que lo afecta.[196] El no otorgar salvaguardas u otorgar algunas que no alcancen este estándar mínimo, defrauda el propósito de imponer algún tipo de control.

A partir de esta sentencia, se ha reiterado en innumerables ocasiones la exigencia del principio de necesidad, entendido a este como una exigencia propia de una sociedad democrática. Entender el principio de necesidad bajo esta perspectiva, implica que toda interferencia debe corresponderse con una apremiante necesidad social, y en particular, que esta sea proporcionada al fin legitimo perseguido.[197] Bajo el parámetro impuesto por esta exigencia, la sola existencia de la amenaza provocada por el terrorismo o los delitos realizados por el crimen organizado, no serían suficiente para permitir la realización de medidas que atentan con el derecho a la privacidad. Se requiere que estas se expresen de forma tal que la sociedad las requiera en su conjunto para asegurar su seguridad.

Sin embargo, la imposición de cualquiera exigencia, sin importar su trascendencia, no puede socavar las prerrogativas propias de las autoridades estatales para determinar, dentro de su margen de apreciación, la forma que han de tomar las actividades de vigilancia.[198]

En definitiva, si bien la justificación de la vigilancia masiva debe responder a una apremiante necesidad social, que reclame la intervención estatal, de igual forma deberá limitarse a las prerrogativas que las autoridades poseen.

2.3.3 Principio de proporcionalidad

Este principio implica el "someter a juicio la pluralidad de intereses contrapuestos y en el cual se trata de hacer prevalecer aquel al cual se le atribuya un mayor valor. De este modo,

[196] Ídem.
[197] Tribunal Europeo de Derechos Humanos. Leander v. Suiza. N° 9248/81. Apéndice 50 Disponible en < https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22leander%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-57519%22]}>
[198] Ídem.

una vez que el medio ha sido afirmado como idóneo y necesario para alcanzar el fin pretendido, se examina si su aplicación no resulta excesiva para el individuo."[199]

El juicio de valor especifico requiere determinar si acaso existe equilibrio alguno entre la limitación de la privacidad y el beneficio obtenido por este, o si, por el contrario, resulta excesivo e inapropiado. El objetivo será alcanzado cuando en caso de permitirse la restricción de la privacidad, esta no se altere en lo que respecta a su núcleo esencial.

El TEDH, al referirse a la proporcionalidad, ha tenido en consideración las características particulares de la vigilancia masiva, en particular las exigencias que esta impone en atención a los avances tecnológicos en base a los cuales esta se ha desarrollado, lo que ha derivado en una revisión a la forma en que es concebido y aplicado dicho principio. Se señala en este sentido, que la proporcionalidad exige como requisito esencial que cualquier injerencia a la privacidad sea justificada en un apremiante interés público, el cual debe ser proporcional al peligro al cual se necesita contrarrestar, así como el daño causado. [200] Enseguida un test de proporcionalidad requiere de la realización de un análisis en atención a los derechos aplicados en el caso en concreto, atendiendo a las particularidades del caso.

Este test de proporcionalidad debe atender a las características propias de la vigilancia masiva, en específico las consecuencias que esta provoca en quien es afectado por esta, toda vez que las injerencias provocadas al derecho a la privacidad con el desarrollo de estas actividades no pueden ser subsanados de forma alguna en especie, sus consecuencias en quien es afectado por ella son irreparables. Por ello, la consideración en abstracto entre ambos derechos, en el análisis del caso particular, debe considerar como esencial para la determinación de la proporcionalidad la existencia de un control externo efectivo ya disponible, para permitir la autorización del uso de la vigilancia masiva.[201]

En cumplimiento de esta exigencia se debe optar por la utilización de aquellos medios de vigilancia menos invasivos, que conlleven un menor perjuicio al sujeto o población

[199] Fuentes Cubillos Hernán. (2008) El Principio de Proporcionalidad en el Derecho Penal. Algunas consideraciones acerca de su concretización en el ámbito de la individualización de la pena. [en línea] Ius et Praxis v.14 n.2 Talca. Disponible en https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-00122008000200002> [Consultado el 28 de septiembre de 2018] p.25.
[200] Ídem.
[201] Idem.

afectada. La utilización de un medio de vigilancia tan lesivo como lo es la vigilancia masiva, en atención al daño irreparable que causa en las garantías fundamentales, solo se justifica cuando otros medios menos invasivos ya han sido utilizados y no cumplen con el propósito perseguido.[202]

La proporcionalidad no se agota en el examen previamente descrito, sino que, por el contrario, abarca en consideración a la extensión de la recopilación y tratamiento de datos, el uso posteriori que estos reciben por parte del agente responsable de su recolección. Este aspecto se considera parte esencial de este criterio, toda vez que, un análisis completo de la actividad de la vigilancia masiva en atención del test de proporcionalidad, no debe atender solamente aquellos bienes involucrados en la etapa inicial de recolección de la información, sino que por el contrario también debe considerar el tratamiento posteriori recibido por estos.

El uso posterior es relevante en cuanto este permite determinar efectivamente quienes tuvieron real o potencialmente acceso a la información. Esto importa reconocer que la información no tan solo es utilizada por agencias de inteligencia estatales para su uso doméstico, sino que puede estar expuesta a al intercambio con otras agencias internacionales, alterando el resultado final del análisis impuesto por el test de proporcionalidad.

Uno de los factores que deben considerarse al determinar la proporcionalidad es que sucede posteriormente con los datos a granel recolectados, y quién pueden acceder a estos una vez recopilados. La justificación ultima de la vigilancia masiva radica en la lucha contra el terrorismo o formas de crimen organizado que amenazan y amedrentan a la población, pero una vez que se permite la práctica de estas actividades, y la información y datos se encuentran disponibles, se pierde todo tipo de control que permita afirmar que el propósito se ha alcanzado o a lo menos perseguido.

En aplicación del principio de proporcionalidad se debe examinar que ocurre con los datos, una vez que estos han sido recopilados, ya que en aplicación de los principios previamente

[202] Idem.

analizados la vigilancia masiva puede considerarse conforme a derecho y necesaria en atención al fin perseguido, pero perder esta calidad si es utilizada para alcanzar otros fines.

CAPITULO III: DERECHO COMPARADO

3.1 Regulación en el Derecho Americano

A nivel americano existe un expreso reconocimiento de la privacidad como derecho fundamental, consagrándose en las distintas legislaciones en concordancia a lo dispuesto por diversos tratados internacionales.

Al igual que en el resto del mundo debido a las revelaciones efectuadas en el año 2013 por Edward Snowden, La vigilancia masiva se ha convertido en una materia de gran relevancia, en atención a potencial para vulnerar derechos fundamentales. A pesar de esto, y a diferencia del caso europeo, existe una escasa regulación de los métodos y prácticas de vigilancia masiva, la cual solamente se encuentra contemplada en los casos de Estados Unidos de Norteamérica y Canadá. En el caso del resto de los países que componen el continente, se presenta al respecto un vacío normativo debido a la falta de regulación en la materia en específico. Sin perjuicio de esto, contemplan en su legislación una serie de normas que autorizan actividades propias de la vigilancia masiva, las cuales tienen por objeto el desarrollo de las actividades de los servicios de inteligencia o de la fuerza policial, en el contexto del desarrollo de la investigación penal.

3.1.1 Brasil

El derecho a la privacidad se encuentra reconocido en el artículo 5° n°10 de la Constitución Federal, la inviolabilidad de la intimidad, la vida privada, el honor y la imagen de las personas, asegurándose el derecho a indemnización por el daño material o moral derivado de su afectación.

Brasil ha sido considerado como uno de los líderes en la regulación del mundo digital, y muestra de esto fue la dictación del "Marco Civil da Internet", la cual pretendida conciliar el desarrollo de las actividades en línea con las exigencias impuestas por el derecho a la privacidad, determinando el uso de internet por la población en general, así como por los proveedores de este servicio.[203]

Esta regulación del área digital, en cuanto al desarrollo de actividades de vigilancia masiva, se complementa con la ley 9.296, las resoluciones 426/05 y 614/13, entre otras normas, que regulan la interceptación, recopilación de información en el desarrollo de una investigación penal.

La Marco Civil da Internet consagra en su artículo 3° como principio rector para el uso de internet el respeto a la privacidad, el cual se manifiesta en su artículo 7° al señalar el carácter esencial del acceso a internet para el ejercicio de la ciudadanía, lo que se deriva en la protección irrestricta de la vida privada, su protección e incluso indemnización en caso de existir daño producto de su violación, así como la inviolabilidad y secreto de las comunicaciones. En adición a esto en la sección segunda se establece que la custodia y entrega de los registros de conexión y de acceso a aplicaciones de Internet de que trata la ley, así como de los datos personales y el contenido de las comunicaciones privadas, deben atender a la preservación de la intimidad, de la vida privada, de la honra y de la imagen de las partes directa o indirectamente involucradas.[204]

En cuanto a la recopilación de la información o datos, esto solo puede realizarse con el consentimiento previo del usuario, y siempre que estos datos solicitados no sean considerados como excesivos en relación con la finalidad que persigue su recolección. Se le

[203] Borges, Bruno y Santoro, Mauricio. (2016) Brazilian Foreign Policy Towards Internet Governance. [en línea] Disponible en <http://www.scielo.br/pdf/rbpi/v60n1/1983-3121-rbpi-60-01-e003.pdf> [Consultado el 2 de junio de 2018] p. 1.

[204] Artículo 10. La custodia y entrega de los registros de conexión y de acceso a aplicaciones de Internet de que trata esta ley, así como de los datos personales Marco Civil Brasileño de Internet 33 y del contenido de las comunicaciones privadas, deben atender a la preservación de la intimidad, de la vida privada, de la honra y de la imagen de las partes directa o indirectamente involucradas.

otorga al usuario de la plataforma el control sobre los datos de su autoría, requiriendo de su parte consentimiento expreso para la recolección.

La vigilancia entendida como interceptación de las comunicaciones, es abordada en diversas disposiciones, las cuales establecen como principio la necesidad de intervención judicial para la autorización de dicha actividad. En específico imponen esta exigencia el articulo 7 en sus numerales II y III[205], así como el Capítulo III de la ley.

La extensión del periodo de tiempo por el cual se permite el almacenamiento de registros de conexión a internet, fue un tema controvertido durante la discusión de la ley. Si bien en la actualidad esta información debe ser almacenada por un periodo de tiempo no inferior a un año, se abogó por establecer un plazo inferior en consideración a la extensión que dichos datos poseen. La importancia de estos registros radica en que permiten identificar el usuario, su IP de conexión, el tiempo de esta, así como otras cuestiones relacionadas con la conexión.[206] La consideración de su importancia se determina por las consecuencias del análisis de dichos datos, los cuales utilizados en su conjunto otorgan un alto poder intrusivo a quien los posea.

3.1.2 Canadá

Al igual que Estados Unidos de Norteamérica, Canadá aprobó producto de ataques terroristas, aprobó el año 2001 la llamada Anti-Terrorism Act, la cual perseguía cuatro objetivos principales, siendo tales prevenir el ingreso del terrorismo al país y de esa manera proteger a la población de actos constitutivos de terrorismo, otorgar herramientas para identificar, procesar, condenar y sancionar el terrorismo; mantener la frontera con Estados Unidos de América segura y contribuir a la seguridad económica, y finalmente, trabajar

[205] II – la inviolabilidad y secreto del flujo de las comunicaciones por Internet, salvo por orden judicial, de acuerdo con la ley; III – la inviolabilidad y el secreto de sus comunicaciones privadas almacenadas, salvo por orden judicial.

[206] Marco Civil Brasileño de Internet, (2015), Centro de Documentación e Información Edições Câmara Brasília. [en línea] Disponible en <https://eva.fing.edu.uy/pluginfile.php/99128/mod_resource/content/1/marco_%20civil%20_internet.pdf> [Consultado el 1 de Octubre de 2018], p.11.

con la comunidad internacional para llevar al terrorismo ante la justicia y atacar la raíz de la violencia.[207]La agencia de inteligencia y ciberseguridad encargada de llevar a cabo las actividades de vigilancia, tiene el nombre de Communication Security Establishment.[208]

Los cuestionamientos realizados a los programas de vigilancia masiva en Canadá se han concentrado en su legalidad en cuanto estos permiten la captura de metadatos emitidos de forma automática por teléfonos celulares, mensajes de textos, entre otros, en consideración a la información que puede ser extraída de esta.

Tal ha sido el cuestionamiento que incluso la Corte Suprema de Canadá se ha pronunciado sobre el particular, refiriéndose a las implicancias de los metadatos en relación a la privacidad, en cuanto permiten la obtención de un sinfín de información que bien puede servir en el contexto del desarrollo de una investigación penal, nada obsta que sea utilizada para acceder a detalles íntimos de la vida de las personas escapando de su propósito original.[209]

Por medio de esta normativa se otorgaban amplios poderes y facultades a las fuerzas policiales como a los servicios de inteligencia para la investigación y persecución del terrorismo. En su cláusula 19 se introducen modificaciones al Código Penal con el objetivo de ampliar los supuestos que habilitan la realización de actividades de vigilancia, las cuales pueden ser llevadas a cabo en determinados casos sin la intervención de autorización judicial.

En el año 2017, se reformó la legislación previamente expuesta por medio de la dictación de la denominada Bill C-59[210], la cual a pesar de su pretensión de corregir todas las

[207] Consultar en <http://www.justice.gc.ca/eng/cj-jp/ns-sn/act-loi.html>
[208]Parsons, Christopher, Lex Gill, Tamir Israel, Bill Robinson, y Ronald Deibert. (2007) Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act respecting national security matters), University of Toronto. [en línea], Disponible en <https://citizenlab.ca/wp-content/uploads/2017/12/C-59-Analysis-1.0.pdf> [Consultado el 2 de Octubre de 2018]. p.3.
[209]Geist, Michael. (2015) Law, Privacy and Surveillance in Canada in the Post-Snowden Era. [en línea] Disponible en <https://press.uottawa.ca/law-privacy-and-surveillance.html> [Consultado el 2 de junio de 2018] p.233.
[210] Puede ser consultado en <http://laws-lois.justice.gc.ca/eng/AnnualStatutes/2015_20/page-7.html#h-29>

deficiencias de la legislación anterior, no logró su cometido. A pesar de que impone determinadas modificadas originadas en las problemáticas de orden constitucional identificados en la normativa que la antecedía, de igual forma intenta legitimar conductas y actividades gubernamentales en materia de vigilancia.[211] En su cuarta parte, en la cual se establecen las enmiendas a la Canadian Security Intelligence Service Act, se introduce un nuevo marco normativo que valida el desarrollo de las actividades de vigilancia masiva. Se permite el uso, retención, análisis y manejo de base de datos, cuando medie una autorización ministerial o judicial.

Una de las cuestiones que ha generado grandes cuestionamientos, es la autorización que se entrega para recolectar cualquier tipo de información que sea considerada como públicamente disponible, lo que permite en el caso en concreto recolectar y analizar la información en cuestión de forma masiva con un nulo control.

En este punto se cuestiona especialmente que la agencia de inteligencia pueda desarrollar actividades de recolección masiva de datos, bajos dos supuestos, los cuales se diferencian sustancialmente en sus requisitos, y por consiguiente, en el control exigido. La regla general, impone la obligación de requerir una autorización judicial para el desarrollo de la vigilancia.[212] A pesar de esto, se permite que la CSE de forma independiente demuestre la necesidad de llevar a cabo actividades de recolección masiva de datos, alegando la ineficacia de los métodos tradicionales, para así obtener una autorización ministerial que permita el desarrollo de la vigilancia, esto en concordancia con la sección 35 de la normativa.[213]

Así, queda en evidencia, que no tan solo se perpetua el desarrollo de las actividades de vigilancia masiva, aun cuando esta ha sido cuestionada. Es más, se plantea la cuestión de la aplicación excepcional de la medida previamente descrita, la cual razonablemente puede

[211] Parsons, Christopher, Lex Gill, Tamir Israel, Bill Robinson, y Ronald Deibert op. cit. p.7.
[212] Parsons, Christopher, Lex Gill, Tamir Israel, Bill Robinson, y Ronald Deibert, ibid. p.17.
[213] Parsons, Christopher, Lex Gill, Tamir Israel, Bill Robinson, y Ronald Deibert, ibid. p.17.

pensarse que será ocupada de forma generalizada como un mecanismo para evadir control respecto de la vigilancia.

Se ha señalado que dos materias son centrales en la revisión de la regulación de la vigilancia masiva, estos siendo, el control y responsabilidad que se ejerce en el modelo actual. Ambas funciones en la actualidad están encargas al comisionado de la CSE, la agencia nacional de inteligencia, lo que deriva en un control poco efectivo del sistema. [214]

A pesar de la preocupación por la extensión de la vigilancia, así como la problemática generada alrededor de los metadatos, el gobierno se ha encargado de señalar que dichos datos carecen de importancia alguna, otorgando autorizaciones que permiten su recolección en la actualidad de manera expedita, atentando directamente contra el resguardo de la privacidad.[215]

3.1.3 Estados Unidos de Norteamérica

Con la publicación del afamado artículo "The Right to Privacy" de Warren y Brandeis[216], se configura inicialmente el derecho a la privacidad en el derecho norteamericano, el cual se caracteriza por la delimitación de un espacio de intimidad ajeno a la intervención de terceros, "the right to be alone". Con el paso del tiempo y a consecuencia de las exigencias impuestas por la sociedad, la Corte Suprema Federal Norteamericana ha derivado en un paso desde un ámbito de protección del derecho a la privacidad basado en el common law, hacia el propio Derecho Constitucional, como consecuencia de la evolución del concepto, desde una visión relacionada con el derecho a la propiedad a una concepción vinculada a la dignidad de las personas. [217]

---

[214] Ídem.
[215] Geist, Michael. op. cit. p.235.
[216] Samuel D. Warren y Louis D. Brandeis (1980) The Right to Privacy [en línea] Harvard Law Review, Vol. 4, No. 5, pp. 193-220. Disponible en < https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf> [Consultado el 16 de diciembre de 2018]
[217] Nieves Saldaña, Maria. (2011) El derecho a la privacidad en los Estados Unidos: Una aproximación diacrónica a los intereses constitucionales en juego. [en línea] Disponible en <http://revistas.uned.es/index.php/TRC/article/view/6960> [Consultado el 25 de mayo de 2018] p. 280.

Las actividades de vigilancia en Estados Unidos de Norteamérica no son una cuestión reciente, sino que, se remontan a inicios del siglo pasado, específicamente a 1919 con la creación de su primera agencia de inteligencia, the Cipher Bureau. Ellos adquieren especial importancia a consecuencia del atentado perpetrado el 11 de septiembre de 2001, en el World Trade Center y el Pentágono, ya que son dictadas como resultado directo de esto la USA Patriot Act o Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act[218], que tiene por antecedente la Foreign Intelligence Surveillance Act (en adelante FISA) de 1978, en el contexto de la llamada guerra contra el terrorismo. Se le otorgaba por medio de esta a los organismos policiales federales y de inteligencia, una serie de facultades y herramientas, para la persecución y prevención del terrorismo. Así es como los instaba a coordinar y cooperar en el desarrollo de sus funciones.

La Patriot Act centraba la labor de las agencias de inteligencia y policiales en las actividades de "prevención" del terrorismo, en contraposición a aquellas destinadas a la persecución de este[219], dotando de mayores facultades de interceptación, recolección y tratamiento de datos a las agencias.

La base del sistema de vigilancia durante la vigencia de la Patriot Act se encontraba su sección 215[220], la cual regulaba el acceso a registros y otros temas bajo la aplicación de la sección 702 de FISA.[221] Estas normas eran las que en definitiva permitían el acceso irrestricto y recolección de información en masa de los ciudadanos estadounidenses. En

[218] El texto completo puede ser encontrado en <https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf>

[219] Whitehead W., John y. Aden Steven. (2002) Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA Patriot Act and the Justice Department's AntiTerrorism Initiatives. [en línea] Disponible en <http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1149&context=aulr> [Consultado el 1 de junio de 2018] p.1083.

[220] Extracto: The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

[221] Suarez, Sergio (2017) Is America Safer? The USA FREEDOM Act of 2015 and What the FBI and NSA Have, Can, and Should be Doing. [en línea] Disponible en <https://scholarship.shu.edu/cgi/viewcontent.cgi?referer=https://www.google.cl/&httpsredir=1&article=1888&context=student_scholarship> [Consultado el 30 de septiembre de 2018]

aplicación de la sección 215, y empleando un programa autorizado por FISA, la NSA podía requerir los registros telefónicos generados en determinadas compañías de telecomunicaciones. Esto se expresaba en que los servicios de inteligencia tenían un registro completo y actualizado de todas las llamadas telefónicas realizadas, así como de su duración, destino y contenido, sin que existiera por parte de los usuarios conocimiento alguno de esto.[222]Una de las secciones más relevantes en cuanto a la afectación del derecho a la privacidad, es la 218, bajo la cual el parámetro para la obtención de una orden de vigilancia se reduce a tan solo exigir la demostración de que un propósito significativo de la vigilancia es el obtener información, sin que ni siquiera se hubiera dado inicio a una investigación criminal.[223]

El conflicto que causa una norma de este tipo, tal como lo ha expuesto la doctrina, es que permite la vigilancia a gran escala, sin requerir a lo menos alcanzar el estándar de causa probable para su autorización,[224] permitiendo que estas actividades sean llevadas a cabo en de forma indiscriminada sin sujeción a control alguno, provocando un desmedro inconmensurable en las personas afectadas, esto en atención a que la violación a una garantía como la privacidad impide su reparo en naturaleza.

Enseguida, la posibilidad de llevar a cabo dichas actividades sin el requerimiento de una causa probable se opone a lo dispuesto a el título III que determina los supuestos bajo los cuales han de llevarse a cabo las escuchas telefónicas. Ello genera una cuestión mayor, toda vez que esta falta de causa probable e inexistencia de una investigación formal se opone a lo dispuesto por la Cuarta Enmienda de la Constitución Norteamericana, la cual establece como requisito para la interceptación de las comunicaciones la existencia de una causa

[222]Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court JANUARY 23. (2014) [en línea], Disponible en https://www.justsecurity.org/wp-content/uploads/2014/01/Final-Report-1-23-14.pdf, [Consultado el 30 de septiembre de 2018]. p. 22.
[223]. Rackow Sharon H (2002) How the USA Patriot Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of "Intelligence" Investigations [en línea] Disponible en <https://www-jstor-org.uchile.idm.oclc.org/stable/pdf/3312949.pdf> [Consultado el 1 de junio de 2018] p.1675.
[224] Rackow Sharon H. ibid. p.1653.

criminal llevada en contra del sujeto afectado, así como la autorización del juez competente bajo el estándar de causa probable.[225]

Por medio de esta ley se autoriza la vigilancia masiva tanto a nivel nacional como internacional por medio de la intervención de las comunicaciones, en el formato que estas se desarrollaran, así como la recopilación y tratamiento de la información proveniente de la plataforma web, existiendo un escaso y en algunos casos nulo control judicial respecto de estas prácticas.

Ilustrativo a este respecto es la sección 216, la cual permite intervenir, grabar o registrar llamadas dirigidas a un teléfono celular o realizadas por este, con el objeto de monitorear comunicaciones electrónicas, dentro de las cuales se incluyen, por ejemplo, correos electrónicos o el historial de búsqueda del servidor. Si bien, en este tipo de casos se requiere de una orden judicial que autorice las actividades previamente descritas, esta no exige para su otorgamiento la existencia de una causa probable, lo que deriva en que tan solo el requerimiento de los funcionarios policiales de esta autorización es suficiente para su otorgamiento, sin que exista control efectivo alguno. Por medio de esta sección se realizan no tan solo actividades de vigilancia respecto de un individuo determinado, sino que esta puede abarcar un gran número de personas.

Además, permitía requerir a las compañías telefónicas los datos y registros telefónicos de sus usuarios, imponiendo la obligación de mantener dicha información por un prolongado periodo de tiempo.

Se introducen igualmente una serie de enmiendas a FISA, las cuales tienen por objeto ampliar el termino por el cual se desarrollan las actividades de vigilancia masiva a nivel internacional, y la necesidad de la obtención de una orden judicial para llevar a cabo actividades de vigilancia.

Todas estas medidas previamente descritas, en conjunto con otras como la autorización para llevar a cabo monitoreo constante respecto de las transacciones comerciales así como de los antecedentes educacionales, han sido considerados como atentatorios al derecho a la

[225] Ídem.

privacidad del cual los ciudadanos son titulares.[226] Es en este sentido, que la Corte Suprema ha reconocido que la Cuarta Enmienda en sí misma no permite la intercepción de las comunicaciones sin orden judicial previa, incluso en aquellos casos que involucren una amenaza a la seguridad nacional.[227]

El 2 de junio del 2015 fue promulgada la USA Freddom Act, la cual reemplaza a la USA Patriot Act, manteniendo casi en su totalidad el contenido de la legislación previa. De igual forma esta nueva regulación innova, al introducir una serie de restricciones en materias como interceptación y recopilación masiva de información, y los presupuestos bajos los cuales la autorización judicial es requerida para llevar a cabo dichas actividades.

En específico, la modificación de la sección 215 permite en la actualidad al gobierno recopilar registro detallados de llamadas solo en el supuesto de cumplir con determinados requisitos, como la existencia de sospecha razonable de que exista relación entre el sujeto que es objeto de la interceptación y, un agente foráneo relacionado con actividades de terrorismo internacional o de preparación de esta.[228] Se ha señalado que la nueva legislación, al normar la controvertida sección 215, continua permitiendo la recolección de datos a gran escala, pero con la salvedad de requerir un requisito en específico, esto es, la razonable sospecha de que el sujeto intervenido este asociado con un agente nacional o internacional vinculado al terrorismo.

Con la modificación legal, si bien las actividades de vigilancia masiva no fueron abolidas en su totalidad, si se limitó las formas en que el gobierno intercepta y recolecta grandes cantidades de información.[229]

3.2 Derecho Europeo

3.2.1 España

[226] Rackow Sharon H ibid., p. 1131.
[227] Rackow Sharon H . ibid. p.1108.
[228] Suarez Sergio op. cit. p.17.
[229] Suarez Sergio op. cit. p.16.

El entramado normativo en España concerniente al derecho a la privacidad adquiere gran relevancia a consecuencia de los avances que se han producido en materia de protección de datos personales durante la última década.

La Constitución española consagra en el art. 18.1 y 18.4 el derecho a la intimidad, el cual se complementa con la normativa sectorial de la UE. Al respecto, se ha entendido por la doctrina que esta garantía tendría por objeto el proteger de cualquier forma de injerencia a este ámbito reservado o privado tutelado por el derecho en comento.[230] Por su parte, el Tribunal Constitucional español ha señalado que la Carta Fundamental garantiza el derecho a poseer la intimidad, más no el contenido abstracto que se entiende la compone, de la que se deriva que esta otorgue a sus titulares "un poder jurídico sobre la publicidad de la información relativa al círculo reservado de su persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público."[231]

La técnica legislativa utilizada, al igual como ocurre en el caso chileno, conjuga el reconocimiento del derecho a la intimidad con otra serie de garantías[232], las cuales si bien se encuentran estrechamente relacionadas con esta, han sido objeto de consagración individual. Esto ha provocado que doctrinariamente se discuta la naturaleza singular o plural de los derechos consagrados en el artículo 18 en relación a la intimidad, lo cual importa establecer si los derechos al honor y a la propia imagen son manifestaciones de este.[233] La doctrina como la jurisprudencia han concluido que cada uno de estos derechos goza de independencia, ya que si bien se encuentran interconectados, son en último término una emanación de la dignidad humana, en la forma de un derecho personalísimo.[234] En efecto, reconocerlos de forma conjunta importa desconocer las particularidades de cada

[230] González San Juan, José Luis. (2015) Jurisprudencia española sobre la protección del honor, la intimidad y la propia imagen en Internet. [en línea] Disponible en < https://www.ibersid.eu/ojs/index.php/ibersid/article/viewFile/4215/3825 > [Consultado el 10 de noviembre de 2018] p.84.

[231] Tribunal Constitucional Español Sentencia 121-2002 de 20 de mayo de 2002 Fundamento 2°.

[232] Artículo 18. 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen

[233] Martínez de Pisón, José. El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional. p.416.

[234]Martínez de Pisón Cavero, José. (1994) La Constitucionalidad del derecho a la Intimidad. [en línea]Derechos y Libertades: revista del Instituto Bartolomé de las Casas. ISSN: 1133-0937. II (3). p. 313—340. Disponible en <https://docs.google.com/viewerng/viewer?url=https://e-archivo.uc3m.es/bitstream/handle/10016/1493/DL-1994-II-3-Pison.pdf> [Consultado el 12 de noviembre de 2018]

uno, desatendiendo el campo de protección en específico que cada uno entrega.[235] En definitiva "lo que sucede es que existe entre ellos múltiples imbricaciones y que no es raro que se aleguen varios derechos –intimidad y honor o imagen– o, incluso, los tres en los recursos de amparo."[236]

La privacidad en cuanto a su relación con la tecnología y, en específico, con la tecnología de la información, se encuentra expresamente reconocida en el artículo 18.4, la cual limita el uso de la informática con el objeto de garantizar el resguardo de la intimidad. Como señala Pérez Luño por medio de esta norma se "trata de impedir que el flujo de datos necesario para el funcionamiento de la sociedad informatizada de nuestro tiempo, se traduzca en una contaminación de los derechos fundamentales que relegue a sus titulares a meros suministradores de datos."[237]

Se entiende que la protección reconocida constitucionalmente a la intimidad recogida en el artículo 18.1 debe expresamente distinguirse de aquel otorgado en el 18.4, en cuanto solo respecto del segundo de estos otorgaría resguardo a los datos personales de forma particular. Se ha señalado en este sentido por el propio TC español que el articulo 18.4 sería la manifestación del reconocimiento constitucional del habeas data, esto es, la faceta informática del derecho a la intimidad.[238] Es más, reconduce esta distinción al fundamento mismo de la protección que otorga cada una de estas garantías al señalar que "a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello el Tribunal Constitucional ha señalado que "el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o

[235] Martínez de Pisón, José. ibid. p.320.
[236] Martínez de Pisón, José. ibid. p.417.
[237] Pérez Luño, Antonio-Enrique. (1981) Informática y Libertad. Comentario al Artículo 18.4 de la Constitución Española. Revista de Estudios Políticos (Nueva Época) Núm. 24, Noviembre-Diciembre 1981. p.35.
[238] Tribunal Constitucional español sentencia 254/1993, de 20 de julio de 1993, fundamento 6°.

íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.””[239]

La falta de regulación expresa en materia de vigilancia masiva deriva en que el análisis en cuestión deba restringirse a la normativa que regula la interceptación de las comunicaciones. Estas actividades pueden ser llevadas a cabo ya sea por la agencia de inteligencia nacional, o por la policía nacional en el contexto de una investigación dentro del proceso penal. En cuanto a la primera de estas, el Centro Nacional de Agencia de Inteligencia creada el año 2002, es aquel autorizado previo control judicial, a desarrollar medidas de vigilancia respecto de comunicaciones postales, telegráficas, telefónicas o de cualquier otra índole, diligencia que podrá extenderse por un plazo máximo de 6 meses. No existiendo norma de excepción, la única forma de autorizar medidas intrusivas seria por medio de este mecanismo.[240]

En cuanto al proceso penal, la Ley de Enjuiciamiento Criminal (en adelante LECRIM) regula en su capítulo V la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos. Esta autorización de acuerdo con el artículo 588 ter, solo podrá ser concedida respecto de ciertos delitos especificados en la misma ley,

[239] Tribunal Constitucional español sentencia 292/2000, de 30 de noviembre de 2011, fundamento 6°.

[240] 1. El Secretario de Estado Director del Centro Nacional de Inteligencia deberá solicitar al Magistrado del Tribunal Supremo competente, conforme a la Ley Orgánica del Poder Judicial, autorización para la adopción de medidas que afecten a la inviolabilidad del domicilio y al secreto de las comunicaciones, siempre que tales medidas resulten necesarias para el cumplimiento de las funciones asignadas al Centro.
2. La solicitud de autorización se formulará mediante escrito que contendrá los siguientes extremos: a) Especificación de las medidas que se solicitan. b) Hechos en que se apoya la solicitud, fines que la motivan y razones que aconsejan la adopción de las medidas solicitadas. c) Identificación de la persona o personas afectadas por las medidas, si fueren conocidas, y designación del lugar donde hayan de practicarse. d) Duración de las medidas solicitadas, que no podrá exceder de veinticuatro horas en el caso de afección a la inviolabilidad del domicilio y tres meses para la intervención o interceptación de las comunicaciones postales, telegráficas, telefónicas o de cualquier otra índole, ambos plazos prorrogables por sucesivos períodos iguales en caso de necesidad.

o cuando los delitos investigados sean de aquellos que se comenten a través de instrumentos informáticos de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

Estas normas descritas son producto de una reforma llevada a cabo el año 2015, la cual tenía por objeto suplir las deficiencias que la LECRIM presentaba en materia de interceptación de los nuevos medios de comunicaciones tecnológicos.

Relevante a este respecto es lo que ocurre en los casos de mensajería instantánea como WhatsApp o de las plataformas de redes sociales como Facebook, toda vez que en conformidad a la Directiva 2013/40 de la UE, se incluye la interceptación de las comunicaciones entre estos sistemas realizados de forma automática entre los equipos utilizados para estos efectos.[241]

Estos requisitos han sido cuestionados por la doctrina; en efecto, respecto del primero de estos se cuestiona la aparente excepcionalidad de la medida basado en los delitos que la hacen procedente, toda vez que múltiples de los delitos tipificados en la LECRIM llevan aparejados una pena igual o mayor a tres años de cárcel. En definitiva, lo que logra este tipo de requisito es generalizar el otorgamiento de este tipo de medida, transformando la excepcionalidad en la regla.[242]

El segundo de los requisitos previamente expuesto, esto es, que el delito hubiera requerido de la utilización de una plataforma tecnológica, ha generado rechazo por parte de la doctrina. La amplitud de dicho requerimiento otorga un amplio margen discrecional al juez que conoce la causa, el cual puede otorgar sin mayor consideración alguna respecto de la idoneidad de la medida la autorización para su realización, permitiendo que en definitiva se intercepten y controlen sin mayor supervisión este tipo de comunicaciones.[243]

---

[241]Cinta Caminals Jordi, Jové. (2015) Las Reformas del Código Penal 2015. [en línea] Disponible en <https://app.vlex.com/#WW/search/jurisdiction:ES+content_type:4/interceptación/vid/573859007> [Consultado el 17 de diciembre de 2018]

[242]Sanjurjo Ríos, Eva Isabel. (2017) Las Conversaciones de WhatsApp como objeto de Investigación y Prueba en el Proceso Penal [en línea] Justicia: Revista de Derecho Procesal. N°1/2017. Disponible en < https://app.vlex.com/#WW/search/jurisdiction:ES+content_type:4/interceptaci%C3%B3n/vid/703952709> [Consultado el 20 de noviembre de 2017]

[243]Sanjurjo Ríos, Eva Isabel. ibid.p.517.

Respecto de toda intervención que requiera de forma habilitante de una resolución judicial, se ha señalado que "como presupuesto habilitante del acto de injerencia, debe valorar el sacrificio particular y concreto que cada modalidad de comunicación implica."[244]

Una cuestión relevante y preocupante a este respecto se produce respecto de la posibilidad de interceptación de datos masivos así como la ubicación por medio del sistema GPS.

Respecto del primero de estos, tal es la interceptación de datos, el peligro al cual se expone a la población tal como lo expresa el Tribunal Constitucional Español radica en que "intromisión no sólo afecta al ámbito de la intimidad constitucionalmente protegido, sino que puede afectar a la esfera más íntima del ser humano, dadas las múltiples funciones de almacenamiento de datos como de comunicación con terceros a través de Internet que posee un ordenador personal."[245]

Como previamente se ha mencionado, respecto de este tipo de medida se requiere de igual forma una autorización judicial que permita su realización, sirviendo esta de garantía frente a los posibles abusos que se puedan cometer. Pero una cuestión importante a considerar es la excepción a esta regla, ya que la referida autorización judicial impuesta para estas medidas, en aquellos casos de urgencia en el cual se alegue encontrarse comprometido un interés constitucional que haga imprescindible la medida, podrá ser adoptada de forma directa por la policía, sin intervención de terceros, y solo dando cuenta posteriormente al juez de esto.[246] Esta autorización excepcional implica cuestionar si esta es tal como se expone, o si en la práctica dado su vago requisito puede ser utilizada de forma generalizada, como la doctrina lo ha expuesto, considerando que no hay criterio alguno para determinar

[244]López-Barajas Perea, Inmaculada (2016) Aplicación de las Tecnologías de la Información y de la Comunicación a la Investigación Criminal: la Reforma de la Ley de Enjuiciamiento Criminal Española de 2015 [en línea] Revista Iberoamérica de Sistemas, Cibernética, e Informática Volumen 13 N° 2, Año 2016. Disponible en < http://www.iiisci.org/journal/risci/FullText.asp?var=&id=CA489BC16> [Consultado el 25 de noviembre de 2018] p.17.

[245] Tribunal Constitucional español, de 7 de noviembre de 2011sentencia 173/2011.

[246]Artículo 588 sexies c. Autorización judicial. 4. En los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida.

que se entenderá por esta urgencia.[247] Es más se ha cuestionado esta situación en cuanto "la amplitud de la excepción legal choca con la intensidad de la injerencia, dados los derechos fundamentales eventualmente afectados, tal y como ha puesto de manifiesto la jurisprudencia y, más en concreto, presenta dificultades en el caso de contenidos vinculados al derecho a la inviolabilidad de las comunicaciones."[248]

Finalmente, una cuestión controvertida se produce respecto de los datos identificativos IMSI[249] o IMEI13[250], ya que estos pueden ser obtenidos por la policía sin que medie autorización judicial previa, siendo esta una excepción a la regla general impuesta por la LECRIM.

Los datos IMSI permiten identificar el número del equipo de comunicación de la tarjeta SIM, y los datos IMEI13 proporcionan acceso a la tarjeta para acceder a la red de comunicación. Si bien, el Tribunal Supremo español al referirse a esta cuestión ha señalado que no se produciría violación alguna a los derechos fundamentales de las personas afectadas, ya que el acceso a estos datos se trataría de actuaciones equivalentes a una labor de vigilancia convencional,[251] esto no sería tal.

Este tipo de datos, también conocidos como metadatos o datos asociados, a pesar de lo que se puede creer, tal como lo hace el Tribunal Supremo Español, son de igual importancia que aquellos que componen la comunicación misma. Así ha sido reconocido

[247]López-Barajas Perea, Inmaculada. (2017) Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos. IDP. Revista de Internet, Derecho y Política [en línea] Revista de los Estudios de Derecho y Ciencia Política Disponible en <http://www.redalyc.org/html/788/78850913006/> [Consultado el 26 de noviembre de 2018]. p.69

[248] López-Barajas Perea, Inmaculada. ibid. p.70

[249]Acrónimo para: International Mobile Subscriber Identity - Identidad Internacional del Abonado Móvil.

[250]Acrónimo para: International Mobile Station Equipment Identity – Identidad Internacional de Equipo Móvil.

[251] A este respecto ha señalado que "no puede aceptar que la captura del IMSI por los agentes de la Guardia Civil haya implicado, sin más, como pretende el recurrente, una vulneración del derecho al secreto de las comunicaciones. No es objeto del presente recurso discernir, entre todos los datos de tráfico generados en el transcurso de una comunicación telefónica, cuáles de aquéllos merecen la protección reforzada que se dispensa en el art. 18.3 de la CE. En principio, ese carácter habría de predicarse, actualizando la pauta interpretativa ofrecida por el TEDH, de los datos indicativos del origen y del destino de la comunicación, del momento y duración de la misma y, por último, los referentes al volumen de la información transmitida y el tipo de comunicación entablada. Y la información albergada en la serie IMSI, desde luego, no participa de ninguna de esas características." Sentencia Tribunal Supremo español Nº 249/2008 de TS, Sala 2ª, de lo Penal, 20 de mayo de 2008.

doctrinariamente, e incluso por el TJUE[252]. Los metadatos no solo permiten obtener información referente al número celular al cual se encuentra abonado el sospechoso, como lo pretende la ley sino que exceden el propósito exclusivo de dar a conocer los datos identificativos de un medio de comunicación por medio del número IMEI. Estos, como fue expuesto previamente, rebasan el valor que se les confiere individualmente, ya que considerados en forma global, en conjunto con otros metadatos, permiten conocer una serie de información relevante, mediante procesos como el de agregación previamente descrito. Tal es su importancia, que incluso permiten conocer la ubicación por medio de GPS, la cual de acuerdo a la LECRIM, debe someterse al régimen general de autorización judicial.

En este sentido se entiende que poseen tal importancia los metadatos, toda vez que estos permiten revelar "patrones, relaciones y comportamientos. Son importantísimos porque justamente con estos datos es con los que mejor se puede clasificar y procesar a los Objetos Informacionales, incluyendo a los agentes la, es decir a los seres humanos."[253]

Así resulta del todo complejo afirmar como lo hace la jurisprudencia española, esta supuesta inocuidad de los metadatos. La geolocalización, registro de llamadas, datos de tráfico, entre otros, es lo que en definitiva la legislación española permite conocer sin mediar autorización judicial alguna. A pesar de que en la doctrina y jurisprudencia no existe mayor discusión al respecto, cabe preguntarse en virtud de lo expuesto, si en definitiva estas normas en su conjunto permiten llevar a cabo actividades constitutivas de vigilancia masiva. De atenderse a los criterios expuestos en la primera parte de esta exposición, debería ser respondido positivamente.

3.2.2 Francia

Los diversos ataques perpetrados en Francia en los últimos años tuvieron por efecto un esfuerzo legislativo orientado a regular las actividades de vigilancia masiva en pos de prevenir futuros ataques.

[252]A este respecto el TJUE dispuso en el caso Schrems que: "se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada."
[253]Olezza, Marina Florencia (2017) Aspectos Epistemológicos de la Infoesfera. Revista Perspectivas Metodológicas /19/Vol. II. p.39.

Es en este contexto que fue dictada la Ley N° 2015-912, también conocida como "Loi relative au renseignement", la cual fue codificada dentro del Código Francés de Seguridad Interna en su Libro VIII, bajo el título de "Inteligencia".

Dicha ley solo permite que los servicios de Inteligencia lleven a cabo operaciones cuando se encuentren comprometidos determinados intereses, tales como, la independencia nacional, la integridad del territorio o la defensa nacional, interés económico, en la prevención del terrorismo o del crimen organizado, entre otros.[254] Por tanto, el derecho a la privacidad solamente podrá ser violado por el Gobierno en aquellos casos en que lo requiera el interés público y sea expresamente permitido por la ley.[255]

Las Agencias de Inteligencia, para poder llevar a cabo operaciones de vigilancia masiva, requieren de una autorización proveniente del Primer Ministro, el cual deberá consultar a una comisión especialmente creada para estos efectos la llamada, CNCTR o Commission National de Contrôle des Techniques de Renseignement. A pesar de esto, las opiniones emitidas por dicha comisión no son vinculantes, lo que permite que en definitiva no exista control efectivo alguno respecto a las decisiones tomadas y que la instancia conformada por esta carezca de valor alguno.

En adición a esto, de lo expuesto se puede extraer acertadamente que no existe intervención judicial alguna en la obtención de una autorización por parte de las agencias de inteligencias de lo previamente expuesto.

En cuanto a la extensión que la vigilancia puede alcanzar resalta la norma contenida en el artículo 852-1, la cual permite extender los sujetos cuyas comunicaciones son interceptadas, a quienes son considerados como personas "cercanos", a aquel sujeto respecto del cual se ha otorgado la autorización para vigilar, siempre que existan razones para creer que pueden proveer información necesaria.[256]

Otra norma controvertida, que permitiría el desarrollo de la vigilancia masiva, es aquella contenida en el artículo 851-3, la que permite la instalación de “cajas negras” en las redes

[254] Articulo L 811-3 del Código de Seguridad de Francia.
[255] Articulo L 801-1 del Código de Seguridad de Francia.
[256] Articulo 852-1 del Código de Seguridad de Francia.

de los servicios de comunicaciones electrónicos, proveedores de internet y de web hosting, con el objetivo de procesar en tiempo real y automáticamente los datos generados, para así detectar cualquier tipo de amenaza terrorista.[257]

La posibilidad de recolección de datos en tiempo real se intensifica aún más, en cuanto el articulo 851-2, 851-3, permite explícitamente la apropiación de metadatos de individuos identificados como amenazas terroristas, presumiblemente de ser relacionados como tal, o quienes pertenezcan a un grupo o sequito de individuos considerados como terroristas.[258]

En consideración a las amplias facultades que fueron entregas por esta ley a las agencias de inteligencia, previo a su promulgación fue sometida al control del Tribunal Constitucional francés. Si bien el Tribunal respaldó el contenido de la ley, permitiendo su posterior entrada en vigencia, de igual forma consideró que dos aspectos de la misma eran contrarios a la Constitución. Estos dos aspectos se relacionaban a la extensión de las actividades de vigilancia así como las circunstancias bajo las cuales eran estas permitidas. Respecto del primero, se declaró como inconstitucional el desarrollo de actividades de vigilancia masiva fuera del territorio francés en atención a la afectación de terceros que no necesariamente están sometidos a la legislación nacional, y en segundo lugar fue declarado inconstitucional el precepto que permitía llevar a cabo la vigilancia sin requerir la autorización del Primer Ministro así como del Comité Nacional de Técnicas de Inteligencia, en el caso de producirse una situaciones de emergencia[259]. En este caso, al no existir una definición estricta de lo que implica un estado de emergencia, permitía que potencialmente el uso de estas herramientas se convirtiera en excesivo y abusivo.[260]

[257] Petición realizada por ASSOCIATION CONFRATERNELLE DE LA PRESSE JUDICIARE and 11 otras asociaciones v. Francia. <https://privacyinternational.org/sites/default/files/2018-09/2017.09.15%20PI%20French%20Surveillance%20Intervention.pdf> p. 2.
[258] Idem.
[259] Cross, Jennifer. (2017) Cybersecurity and the rights of the internet user in France. [en línea] Disponible en <http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=2400&context=gjicl> [Consultado el 16 de diciembre de 2018] p.614.
[260] A este respecto la falta de autorización por "emergencia" no aludía a la denominada "emergencia constitucional", e incluso no se especificaba que se entendía por tal. Así, se señala que: "The Constitutional Court was concerned that what qualified as an "emergency" situation was not defined and could potentially result in executive abuse."

3.2.3 Gran Bretaña

Gran Bretaña presenta uno de los casos insignes en la materia, toda vez que ha implementado una serie de legislaciones en un esfuerzo por regular la vigilancia masiva. A pesar de esto, la normativa respectiva presentaba una serie de deficiencias en materia de derechos humanos, específicamente en lo concerniente al derecho a la privacidad. Como consecuencia de esto recientemente esta fue dejada sin efecto por medio de una sentencia emanada de la Court of Appeal.[261]

Gran Bretaña aprobó en el año 2014 la llamada Data Rentention and Investigatory Act, la cual fue reforzada en el año 2016 por medio de la aprobación de la Investigatory Power Act. Ambos cuerpos normativos de forma conjunta establecen el régimen de vigilancia masiva a regir en el país, el cual otorga amplias facultades de vigilancia, en conjunto con amplios periodos de retención de la información obtenida, así como un casi nulo control judicial respecto de las actividades de vigilancia realizadas.

La Investigatory Power Act prohíbe en su sección 63[262] que el oficial superior a cargo de una investigación apruebe una autorización que permita la utilización de los métodos de vigilancia descritos en la ley, cuando se encuentre trabajando en el caso en cuestión. A pesar de esto, excepcionalmente el mismo oficial superior puede otorgar dicha autorización en aquellas investigaciones en que el mismo intervenga cuando, existan circunstancias excepcionales que así lo requieran.[263] Queda de manifiesto como la excepción se puede volver la regla general, permitiendo que sin control judicial alguno, se cometan acciones de carácter intrusivo, que pueden atentar e incluso violar el derecho a la privacidad.

Se permite, además, en la sección 106 que un "law enforcement chief", a petición de un subalterno, emita una orden interceptar las comunicaciones en determinados supuestos, que este mismo debe precisar si aplican al caso en concreto. En específico, lo que permite dicha

[261]Consultar en < https://www.judiciary.uk/judgments/secretary-of-state-for-the-home-department-v-david-davis-mp-and-others/>

[262] Sección 63, subsección dispone, (2) But, if the designated senior officer considers that there are exceptional circumstances which mean that subsection (1) should not apply in a particular case, that subsection does not apply in that case.

[263] Examples of exceptional circumstances include- a) an imminent threat to life or another emergency, among others.

norma es la autorización sin intervención judicial alguna de actividades de vigilancia altamente intrusivas que, afectando los derechos fundamentales de la población, pueden ser usadas de forma indiscriminada por cualquier autoridad policial a su antojo.

La Power Act a raíz de lo previamente expuesto generó un amplio rechazo, el cual se sustentaba en el hecho de que la legislación vigente claramente atentaba contra el derecho a la privacidad, al otorgar tan amplias facultades para vigilar de forma generalizada.

Como consecuencia de esto, Tom Watson vicepresidente del Partido Laborista, en conjunto con la Organización No Gubernamental Liberty acudieron al Tribunal de Apelación Británico[264], el cual el 30 de enero de 2018 determinó que determinadas disposiciones contenidas en la Investigatory Power Act eran ilegales, y, por consiguiente requería, de una serie de modificaciones.

La Corte declaró que la sección primera de la Data Retention and investigatory Act era inconsistente con la ley de la Unión Europea hasta el punto que, para el propósito de prevención, investigación, detección y persecución de los hechos delictivos, permite el acceso a información retenida; (a) cuando el objetivo perseguido en virtud del acceso, no estaba exclusivamente restringido a combatir crímenes serios; (b) donde el acceso no estaba sujeto a una revisión previa de un tribunal o una autoridad administrativa independiente.[265]

Esta declaración denominada "declaratory relief", tuvo por efecto inmediato un cambio sustancial en las materias en que se ha declarado como ilegal la ley.

En una segunda ocasión, el TEDH al conocer del caso Big Brother watch and others v. The United Kingdom, se ha pronunciado respecto a las actividades de vigilancia masiva llevadas a cabo por el gobierno británico. En esta oportunidad el pronunciamiento, en relación al derecho a la privacidad, se realiza respecto de la sección 8(4) de RIPA[266], la cual

[264] Court of Appeal (Civil Division), Case No: C1/2015/2612 &2613, January 1 2018.
[265] Section 1 of the Data Retention and Investigatory Act 2014 was inconsistent with EU law to the extent that, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, it permitted access to retained data.
(a) where the object pursued by that access was not restricted solely to fighting serious crime; or
(b) where access was not subject to prior review by a court or an independent administrative authority.
[266] El Tribunal señala a este respecto que"Bulk interception" of communications is carried out pursuant to a section 8(4) warrant. Section 8(4) and (5) of RIPA allows the Secretary of State to issue a warrant for "the

al permitir la interceptación masiva de las comunicaciones, violaría el derecho a la privacidad consagrado en el artículo 8° de la CEDH de acuerdo a lo alegado por los requirentes.

Tal como se ha mencionado, se le reconoce a Gran Bretaña la prerrogativa para determinar las actividades de vigilancia nacionales, restringiéndose el cuestionamiento a la lesión que estas podrían infringir en la privacidad de la población. [267]

La interferencia y su fundamento solo podrá condecirse con la ley de acuerdo al criterio establecido por el mismo tribunal, esto es, cuando persiga uno o más fines legítimos y sea considerada como necesaria en una sociedad democrática. En el caso en específico, dicho requisito se analiza en atención a si RIPA, otorga adecuadas y efectivas salvaguardas y garantías en contra de posibles abusos cometidos por la misma.

El análisis efectuado para determinar la concurrencia de estos requisitos se centra en la extensión de acceso que otorga la normativa en cuestión, la cual permite conocer e identificar todas las comunicaciones y datos de la población., aun cuando la normativa lo restringe a datos en específico.[268]Al respecto, el tribunal considera de especial relevancia que las agencias de inteligencia puedan acceder a los "datos de comunicación relacionados" sin aparente restricción alguna, ya que estos permiten conocer una significante cantidad de datos relevantes de forma irrestricta.[269] Estos datos a pesar de lo señalado por el gobierno británico, serian de igual identidad en cuanto a su relevancia en materia de inteligencia, en comparación a aquellos que explícitamente se refiere la ley. De esto se deriva, en definitiva, que para el TJUE la normativa falla en alcanzar un equilibrio entre el interés público y

---

interception of external communications in the course of their transmission by means of a telecommunication system". At the time of issuing a section 8(4) warrant, the Secretary of State must also issue a certificate setting out a description of the intercepted material which he considers it necessary to examine, and stating that he considers the examination of that material to be necessary for the reasons set out in section 5(3) (that is, that it is necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or for safeguarding the economic well-being of the United Kingdom)."
Es la abreviación utilizada para referirse a Regulation of Investigatory Power Act.

[267] Tribunal Europeo de Derechos Humanos, Weber y Saravia con Alemania. Op. cit. apéndice 106.

[268]La sección 8(4) y 16 autoriza a los servicios de inteligencia recolectar no tan solo el contenido de la comunicación de la población intervenida, sino que además, los denominados datos de comunicación relacionados. Esto en definitiva permite acceder a toda la información y datos disponibles de una persona en línea.

[269] Tribunal de Justicia de la Unión Europea, Big Brother Watch y otros, v. Reino Unido, ibid. apéndice 357.

privado, al exceptuar a los "datos de comunicación relacionados", de toda garantía aplicable al registro y examen de contenido sujeto a vigilancia.[270]

El TJUE concluyó que el régimen de vigilancia establecido por la sección 8(4), no se condecía con la exigencia de "calidad de la ley" y es incapaz de mantener la actividad de "interferencia" a lo que es "necesario en una sociedad democrática"[271]. Declaró, en conclusión, que la normativa en cuestión es contraria al convenio y, por tanto, viola el derecho a la privacidad consagrado en este.

3.2.4 Unión Europa

A nivel europeo, la vigilancia masiva es una cuestión que ha cobrado especial relevancia como consecuencia de los múltiples ataques terroristas perpetrados en los últimos años, lo que ha derivado en un gran esfuerzo normativo por regular.

La Convención Europea de Derechos Humanos, así como por la Carta Europea de Derechos Humanos y el Tratado Europeo de Derechos Humanos, reconoce el derecho a la privacidad, concibiendo a este como el derecho que le asiste a todos los sujetos en consideración al respeto que se le debe a su vida privada, así como la familiar, su hogar y correspondencia. La extensión y alcance de este derecho ha sido definido vía jurisprudencial por medio de la labor realizada por el Tribunal Europeo de Derechos Humanos.

El reconocimiento del derecho a la privacidad, en su faz digital, se ha complementado con la protección de los datos personales, la cual se encuentra reconocida en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea. La regulación en materia de datos personales en la Unión Europea, es considerada como la más completa a nivel mundial, dictándose en los últimos años la Directiva 2016/680 y la Regulación 2016/679.

Recientemente el Parlamento Europeo se ha manifestado en la materia, expresando preocupación por el desarrollo de actividades de vigilancia masiva en particular por los Estados miembros, así como por el intercambio de información recolectada que estos llevan

[270] Ídem.
[271] Ídem.

cabo.[272] A este respecto, se ha señalado que los Estados europeos miembros de la UE que poseen u utilizan programas de vigilancia masiva, ponen en peligro el cumplimiento al principio consagrado en el artículo 4.3 del Tratado de la Unión Europea, esto es, la sincera cooperación, ya que por medio de estas acciones comprometen en un doble sentido al Tratado. En primer lugar, ya que la información obtenida y compartida entre los Estados a raíz de la vigilancia masiva es contraria a los regímenes de vigilancia legalmente consagrados, y en segundo lugar, en cuanto se atenta contra la seguridad misma de la UE al utilizar estos métodos.

Una cuestión de extrema importancia es que, bajo la regulación europea, los sujetos son considerados dueños de sus datos o información[273], de lo cual se deriva la ilegalidad que puede representar el acceder y recopilar datos, sin el conocimiento ni menos la autorización de la persona afectada.

La cuestión a nivel de la UE se presenta en dos niveles, el primero referido a la vigilancia masiva realizada por los Estados respecto de sus ciudadanos, y el segundo, referido al intercambio de esta información entre estados miembros.

Del examen que se puede realizar de los diversos proyectos o leyes que actualmente rigen en cada país, queda de manifiesto como la tendencia que opera es a otorgar las más amplias facultades posibles a las policías o servicios de inteligencia, para llevar a cabo actividades de vigilancia masiva.

En cuanto al primer nivel de la problemática, esto es, la regulación a nivel estatal, el TEDH se ha pronunciado en reiteradas ocasiones, señalando que la decisión de adoptar programas

[272]Resolución del Parlamento Europeo, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior. [en línea] Disponible en < http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//ES> [Consultado el 16 de diciembre de 2018]

[273] Bigo, D.; Carrera, S.; Hernanz, N.; Jeandesboz, J.A.; Parkin, J.; Ragazzi, F.; Scherrer, A. (2013) National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law. [en línea] Disponible en < https://dare.uva.nl/search?identifier=95882891-5efc-4211-b502-6da9080e9509> [Consultado el 24 de abril del 2018] p.27.

que resulten en la interceptación masiva de datos compete de forma exclusiva al Estado contratante.[274]

Respecto al segundo nivel, a saber, el intercambio de la información obtenida por medio de vigilancia entre los Estados miembros, el Tribunal de Justicia de la Unión Europea se ha pronunciado, en una sentencia que ha sido considerada como el mayor precedente en la materia. Si bien en esta sentencia el pronunciamiento recae en el intercambio de información con un país no miembro de la Unión Europea, Estados Unidos de América, su pronunciamiento ha sido considerado como el pilar fundamental en materia de protección de derechos fundamentales en el contexto de intercambio de información transfronteriza, en relación con la protección del derecho a la privacidad y de datos personales.

En el denominado caso "Schrems"[275] el TJEU discurre respecto a si la transferencia de datos desde la UE a un Estado no miembro, de acuerdo a lo dispuesto en el acuerdo Puerto Seguro materializado en la Decisión 200/520/CE, era conforme a los estándares de protección que otorga la normativa propia de la UE, en relación al derecho a la privacidad, así como de otros derechos fundamentales. Esto, a consecuencia de que uno de los requisitos de validez de dicha Decisión radicaba en que los estándares de protección otorgados por dicho país fueran similares a los de la UE.

En relación al análisis que incumbe a este trabajo, el TJEU, al referirse al derecho a la privacidad, considera que este ha sido vulnerado en su contenido esencial en cuanto "una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental de respeto a la vida privada."[276] Lo relevante de dicha determinación radica en que esta se constituye en un precedente en la materia, toda vez que altera el criterio impuesto previamente en la sentencia Digital Rights Ireland[277]. De esta manera, la consideración de que el núcleo esencial del derecho a la privacidad se extiende a la

[274] Tribunal Europeo de Derechos Humanos Big Brother watch and others v. The United Kingdom, Applications nos. 58170/13, 62322/14 and 24960/15), 13 de septiembre de 2018 Apéndice 387.
[275] Los hechos pueden ser revisados en <http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES>
[276] Tribunal de Justicia de la Unión Europea Caso Schrems 6 de octubre de 2015 cit. 94.
[277] Este criterio será tratado en extenso posteriormente.

interceptación de la comunicación en su conjunto, sin distinguir a esta de su contenido, permite una protección y resguardo integral de la garantía. Esta consideración es de extrema relevancia, ya que el TJEU se desatiende de la aplicación del test de proporcionalidad impuesto por la CDFUE, restringiendo el análisis de validez de la normativa a la sola determinación de vulneración del núcleo esencial.

Enseguida, el análisis realizado en torno a la equivalencia de protección otorgado por los Estados Unidos de Norteamérica en relación al estándar de la UE, se señala que este es sustancialmente inferior, no ajustándose a los requerimientos establecidos en la Directiva, por lo que permitir niveles de protección menores implica posibilitar la injerencia y transgresión de derechos fundamentales.[278]

[278] Maria Isabel y Sferraza Taibí Prieto. op. cit. p. 226.

CAPITULO IV: EL ESTADO DE LA VIGILANCIA MASIVA EN CHILE

5.1 Casos en que se permite algún tipo de vigilancia

Si bien nuestra legislación no se ocupa directamente de la vigilancia masiva, existen una serie de normas que regulan la intromisión a la privacidad en el contexto del desarrollo de la investigación penal, las cuales podrían permitir la intervención en masa de las comunicaciones y registros online de la población.

5.1.1 Código Procesal Penal

El Código Procesal Penal (en adelante CPP) trata en los artículos 219 y siguientes las denominadas medidas intrusivas, las cuales permiten acceder a las distintas formas de comunicaciones como a otros datos relacionados a estas.

Se establece como principio rector de estas medidas al igual de cualquier otra que signifique privar, restringir o perturbar el ejercicio de cualquier derecho que la Constitución confiere, la existencia previa de una autorización judicial. Este se conoce como el principio del control previo de afectación de derechos, y en definitiva, tal como se ha reconocido doctrinariamente, se ha establecido como una forma de resguardar las garantías individuales consagradas en la Constitución, frente a las medidas intrusivas que se puedan desarrollar durante el proceso.[279]

Al referirse a esta materia el TC ha señalado que "para resguardar los derechos fundamentales (…), el legislador ha establecido en los casos excepcionales que así lo permiten, y sólo por ley, un acucioso procedimiento de apertura y registro de las comunicaciones, procurando, además, que un órgano jurisdiccional vele por las garantías del afectado."[280]

El articulo 218 permite la retención e incautación de correspondencia postal, telegráfica o de otra clase, en los casos que medie una petición fundada por parte del fiscal, la cual debe

[279] Gandulo R.Eduardo. (1999) Principios de Derecho Procesal en el Nuevo Sistema de Procedimiento. Revista de Derecho de la Universidad Católica de Valparaíso XX Valparaíso, Chile. p.439.
[280] Tribunal Constitucional, sentencia rol N° 2246-2012, 31 de enero de 2013.

ser autorizada por un juez. Al realizar una exposición meramente enunciativa, se permite la extensión de los tipos de correspondencia susceptible de incautación, pudiendo incluirse toda aquella proveniente de medios electrónicos. En concordancia con esto en el mismo artículo permite la obtención de copia o respaldo de correspondencia electrónica que sea dirigida al imputado o que en su defecto emane de este.

A diferencia del artículo 222 del CPP que posteriormente se analizará, esta norma establece como único requisito de procedencia la autorización del juez de garantía. La falta de exigencias en atención a la naturaleza del delito o al fundamento de la petición realizada por el fiscal, permite que, en definitiva, esta decisión quede entregada al mero arbitrio del juez de garantía. Esto es problemático, toda vez que, autorizar una medida intrusiva bajo un estándar tan laxo como el descrito, crea un contexto propicio para que los "derechos se debiliten, pues su efectivo ejercicio depende del albur de decisiones imprevisibles y del peso que se asigne a consideraciones diversas de los argumentos jurídicos."[281]
La interceptación de las comunicaciones telefónicas así como de otras formas de telecomunicaciones, se regula en los artículos 222 y siguientes, los cuales permiten tanto la interceptación como la grabación de dichas comunicaciones. Para lograr esto se le impone al proveedor de servicios de telecomunicaciones la obligación de proveer todas las facilidades para realizar dichas diligencias, para lo cual deberá confeccionar un registro actualizado de sus rangos autorizados de direcciones IP, así como un registro de los números IP de las conexiones que realicen sus usuarios, el cual no podrá ser inferior al plazo de un año.

Estas medidas solo pueden afectar al imputado y terceros, ya sea que estos faciliten el medio de comunicación al imputado, o existan sospechas fundadas de que estos sirven de intermediarios a las comunicaciones realizadas por este.

Una cuestión esencial en este punto son las obligaciones que se imponen a los proveedores de servicios de telecomunicaciones, en específico, cierta información que estos deben

[281] Weezel van, Alex - Darricades, (2011) Tomás, Interceptaciones telefónicas. Oportunidad para avanzar, en Revista del Abogado del Colegio de Abogados de Chile, 52, (julio de 2011), pp. 40-43. p.42.

almacenar y entregar respecto de sus usuarios. La determinación de estos datos se constituye como la regla general. En primer lugar, las empresas deberán mantener en carácter reservado un listado actualizado de sus rangos autorizados de dirección IP, lo que permitirá identificar con exactitud a sus clientes. Además, estos deberán llevar un segundo registro, el cual deberá remontarse a lo menos en un año respecto de los números IP de todas las conexiones realizadas por los usuarios. Ambos listados deberán ser confeccionados para el caso de que el Ministerio Publico requiera de ellos, encontrándose a su plena disposición.

Los criterios establecidos por la ley para autorizar esta diligencia no son del todo pacíficos, generando disimiles posiciones en la doctrina. Una parte de esta, sustentada en específico por el ente persecutor, esto es, el Ministerio Público, estima que el estándar impuesto es innecesariamente alto. Funda su posición en que el nivel de exigencia de una resolución de naturaleza temporal, revocable y revisable como es la que autoriza la intercepción, no debería ser igual a aquellas de carácter definitivo como lo es el de una sentencia definitiva.[282] Es más, señalan que tal grado de exigencia deriva en que la investigación carezca de sentido, ya que al requerir las pruebas necesarias para establecer el hecho punible así como la participación del imputado, nada habría que probar en un posterior juicio.[283]

La doctrina contraria, en cambio, estima que estos requisitos son innecesariamente amplios, recayendo en definitiva el otorgamiento de la autorización en "el juicio de mérito sobre el carácter "imprescindible" de la medida, así como sobre la presencia o no de "fundadas sospechas, basadas en hechos determinados"[284]que el juez realice. En efecto, la cuestión se vuelve aún más problemática cuando se considera que la decisión del juez es tomada sin que necesariamente este conozca de los antecedentes de la causa, al no establecerse dicho

[282] Ivelic Mancilla, Alejandro. (2014) Las Interceptaciones de Comunicaciones Telefónicas en los Delitos de Tráfico Ilicito de Estupefacientes. Revista Jurídica del Ministerio Público, N° 60. p.112.
[283] Ídem.
[284] Weezel van, Alex - Darricades, op. cit. p.41.

requisito en la ley. Esto deriva en que su función, se limite a "hacer fe" de que no existen antecedentes contrarios bajos los cuales toma su decisión.[285]

Adscribir a la primera de las posturas expuestas atenta contra el respeto y protección garantizado en nuestra Constitución a los derechos fundamentales, en específico, la privacidad. Las medidas intrusivas consagradas dentro del proceso penal son excepcionales, toda vez que importan la lesión de garantías fundamentales, por lo que el control previo de afectación de derechos es un imperativo. Desconocer este mínimo legal contraría lo dispuesto en la misma ley, así como en la Constitución, en aplicación del irrestricto respeto de los derechos fundamentales, el cual como imperativo derivado de la observancia del principio de supremacía constitucional obliga a todos los órganos del Estado.[286]

5.1.2 Ley N°19.974 sobre el Sistema de Inteligencia del Estado y crea la Agencia Nacional de Inteligencia

La ley N° 19.974, se encarga de definir los lineamientos bajos los cuales toda actividad de inteligencia o contrainteligencia, serán llevadas a cabo, con el objetivo de proteger la soberanía nacional y preservar el orden constitucional. Es así como el Título I de esta ley, encargado de establecer los principios bajo los cuales han de desarrollarse dichas actividades, define y sustenta su función.

Establece en su Título II que estas actividades serán llevadas a cabo de forma exclusiva por agencias de inteligencia policial y militar, los cuales deberán por medio de las facultades que se otorgan en la ley combatir el terrorismo, el crimen organizado y el narcotráfico a nivel nacional.

Se deriva de esto, que la ley sustenta el actuar de las agencia así como la entrega y el ejercicio de las facultades en ella previstas, por un lado, en la protección y preservación de la soberanía nacional como el orden constitucional, como en el combate contra el terrorismo, el crimen organizado y el narcotráfico a nivel nacional. Dichos fines a pesar de estar solamente enunciados en la ley, no encuentran definición en esta, permitiendo un

[285] Ídem.
[286] Navarro, Enrique y Carmona Carlos op. cit. p.87.

amplio margen de discrecionalidad para la determinación de su procedencia en el caso en concreto.

En cuanto a las actividades de vigilancia, en el Título V denominado "Los procedimientos especiales de obtención de información", se establecen los parámetros bajo los cuales se han de desarrollar aquellas actividades que tienen por consecuencia la transgresión de derechos fundamentales, como la privacidad., determinándose en este respecto los supuestos bajos los cuales dichas acciones pueden ser permitidas, así como los distintos medios que han de utilizarse.

A este respecto señala el artículo 23: " Cuando determinada información sea estrictamente indispensable para el cumplimiento de los objetivos del Sistema y no pueda ser obtenida de fuentes abiertas, se podrá utilizar los procedimientos especiales de obtención de información a que se refiere el presente Titulo, en la forma y con las autorizaciones que en el mismo se disponen."

Se establecen como requisitos primordiales para el acceso de todo tipo de información que, en primer lugar, esta tenga el carácter de indispensable para el desarrollo de las actividades de las agencias de inteligencia, y como segundo, que exista una imposibilidad de obtenerla por medio de fuentes abiertas. Queda en evidencia como dichos requisitos, en especial el primero de estos, permiten un alto grado de discrecionalidad a quien corresponda calificarlo, toda vez que bajo determinadas circunstancias cualquier tipo de información, sin importar lo insignificante que sea, puede ser considerada como indispensable.

En concordancia con dicho argumento, se establece el control judicial, el cual es ejercido por un ministro de la Corte de Apelaciones competente en consideración al territorio jurisdiccional en el cual se realice la diligencia, o se dé inicio a esta, el cual deberá determinar si concurren los requisitos, y, por consiguiente, si se otorga la autorización judicial respectiva.

El artículo 24, en particular, establece que se entiende por esta “los antecedentes relevantes contenidos en fuentes cerradas o que provienen de ellas, que aporten antecedentes necesarios al cumplimiento de la misión especificada de cada organismo operativo.”

Los procedimientos por los cuales se permite acceder a dicha información son:

a) La intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia
b) La intervención de sistemas y redes informáticos
c) La escucha y grabación electrónica incluyendo la audiovisual, y
d) La intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información.

A pesar de que de un análisis superficial se pueda señalar que dichos procedimientos se encuentran agotados en lo establecido en el artículo 24, la letra d) contenida en este permite que la implementación como el desarrollo de cualquier tipo de procedimiento que permita el alcance de los objetivos establecidos en la ley.

El artículo 27 de la ley establece que el Director de la Agencia podrá disponer del uso de los procedimientos especiales previamente descritos, con la autorización judicial correspondiente, siempre que se encuentre en el ejercicio de las funciones del artículo 8° letra f) y g).[287] Y por consiguiente, la autorización judicial requerida por el Director de la Agencia queda en definitiva determinada por su arbitrio, en aquellos casos en que se esgrima la letra f), esto es, cuando la aplicación de las medidas de inteligencia se utilice para el combate del terrorismo. En este caso la discrecionalidad del Director es mayor en atención a lo dispuesto por la ley, pudiendo exigir la autorización de medidas altamente intrusivas y extendidas constitutivas de vigilancia masiva. Cabe destacar que esta mayor discrecionalidad solo tiene lugar cuando se alude al combate del terrorismo, y no en los casos del crimen organizado.

5.1.3 Ley N° 18.314 que determina las conductas terroristas y determina su penalidad

[287] Artículo 8º.- Corresponderán a la Agencia Nacional de Inteligencia, en adelante la Agencia, las siguientes funciones:
f) Disponer 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.
g) Disponer la aplicación de medidas de contrainteligencia, con el propósito de detectar, neutralizar y contrarrestar las actividades de inteligencia desarrolladas por grupos nacionales o extranjeros, o sus agentes, excluyendo las del inciso segundo del artículo 20.

Tal como se desprende de su nombre, esta ley se encarga de la persecución de las conductas terroristas, así como de la determinación de su sanción. Se establece en el artículo 1° que tendrán el carácter de delitos terroristas, aquellos que se cometan con la finalidad de producir en la población o en una parte de esta, un temor injustificado a ser víctima de dichos delitos de ser víctima de delitos de la misma especie, sea por la naturaleza y efectos de los medios empleados, sea por la evidencia de que obedece a un plan premeditado de atentar contra una categoría o grupo determinado de personas, sea porque se cometa para arrancar o inhibir resoluciones de la autoridad o imponerle exigencias.

Inmediatamente en el artículo 2° señala una serie de conductas constitutivas de delitos de terrorismo, cuando estas cumplan con la exigencia expuesta previamente, esto es, la de infundir temor injustificado de ser víctima de estos delitos. Entre estos delitos se encuentran el homicidio contemplado en el artículo 391 del Código Penal, el atentado contra la vida o integridad corporal del Jefe de Estado, entre otros.

Ahora bien, respecto de las intromisiones que se autorizan en aplicación de la ley, estas se encuentran contenidas en su totalidad en él artículo 14. Se autoriza al Ministerio Publico con previa autorización del juez de garantía interceptar, abrir o registrar las comunicaciones telefónicas e informáticas y su correspondencia epistolar y telegráfica. Cabe destacar la distinción que se realiza respecto del tipo de comunicación interceptada, toda vez que estas son agrupadas bajo los términos “telefónicas e informáticas” y “correspondencia epistolar y telegráfica”. La ley señala además, que solo podrán ser intervenidas las comunicaciones telefónicas e informativas, excluyendo por tanto, otro tipo de comunicaciones contemplados en la Ley N° 19.974, como las radiales. A este respecto, el término utilizado por la ley es relevante en cuanto este restringe la intervención a las llamadas “comunicaciones informáticas”, las cuales no son definidas por esta misma, dejando este asunto a la determinación alcanzada caso a caso por el juez correspondiente.

A pesar de esto, el inciso segundo del articulo 14[288] amplía las diligencias permitidas en este tipo de casos, autorizando la práctica de aquellas consagradas en el artículo 236[289] del CPP. Estas nuevas actividades no son otras que las previamente tratadas al referirnos al CPP, pero con la particularidad de que estas se llevaran a cabo sin el conocimiento previo del afectado. El desconocimiento de la realización de las diligencias, si bien puede ser considerada como una cuestión fundamental para el desarrollo del proceso, de igual forma podría permitir un mayor riesgo a cualquier tipo de vulneración de garantías fundamentales relacionadas con el desarrollo de la investigación.

5.2 Operación Huracán

Dentro del contexto del llamado "Conflicto Mapuche", en septiembre de 2017, se llevaron a cabo una serie de detenciones en contra de comuneros mapuches, la cuales encontraban su origen en la investigación realizada por parte de Carabineros de Chile en directa aplicación de la Ley de Inteligencia.[290] Esta investigación se presentaba como una experiencia exitosa en la utilización de la legislación de inteligencia a nivel nacional, permitiendo el uso de herramientas tecnológicas de punta en el combate contra asociaciones terroristas.

El actuar de Carabineros se sustentaba en la aplicación de la Ley N°19.974, así como el Reglamento sobre Interceptación y Grabación de Comunicaciones Telefónicas y de otras formas de Telecomunicaciones 142 de 2005, los cuales permitían la interceptación de las

[288] Artículo 14, inciso 2°: "(…) Sin perjuicio de lo anterior, en cualquier momento el Ministerio Público podrá solicitar autorización judicial para la realización de diligencias de investigación que la requieran, en los términos del artículo 236 del Código Procesal Penal."

[289] Artículo 236.- Autorización para practicar diligencias sin conocimiento del afectado. Las diligencias de investigación que de conformidad al artículo 9º requirieren de autorización judicial previa podrán ser solicitadas por el fiscal aun antes de la formalización de la investigación. Si el fiscal requiriere que ellas se llevaren a cabo sin previa comunicación al afectado, el juez autorizará que se proceda en la forma solicitada cuando la gravedad de los hechos o la naturaleza de la diligencia de que se tratare permitiere presumir que dicha circunstancia resulta indispensable para su éxito.

Si con posterioridad a la formalización de la investigación el fiscal solicitare proceder de la forma señalada en el inciso precedente, el juez lo autorizará cuando la reserva resultare estrictamente indispensable para la eficacia de la diligencia.

[290]Esta noticia recoge la versión originalmente entregada a la prensa. Disponible en < https://tn.com.ar/politica/prision-preventiva-para-ocho-mapuches-imputados-por-asociacion-ilicita-terrorista_822577>

comunicaciones de los sospechosos por medio de cualquier medio considerado como idóneo para esos efectos, y a su vez la retención de las comunicaciones por un periodo prolongado de tiempo, para ser estas requeridas y utilizadas en el desarrollo de la investigación.

Dado que el alcance de dichas medidas, las cuales solo afectaron a ocho individuos, no puede calificarse el caso en cuestión como uno que implique vigilancia masiva propiamente tal. Esencial para esta calificación es la naturaleza limitada y selectiva de las medidas tomadas, las cuales de ninguna manera intentaron rebasar el ámbito especifico de los comuneros investigados. Pero de igual forma nos permite vislumbrar cuestiones relevantes al pensar en el despliegue de esta actividad a nivel nacional. Así, se vuelve relevante reflexionar respecto del uso de medidas intrusivas, en específico, aquellas necesarias producto del avance tecnológico su alcance y los peligros que en este caso se evidenciaron.

Tal como lo destacaron múltiples medios de prensa a nivel nacional, esta operación buscaba combatir una serie de atentados terroristas perpetrados en la región de la Araucanía, lo cual requería según las policías a cargo de las investigaciones de estos delitos, del despliegue de todas las herramientas que la Ley prevé para el desarrollo de su función.

Para estos efectos se creó por Carabineros la Unidad de Inteligencia Operativa Especial (UIOE),[291] la cual al amparo de la Ley de Inteligencia N° 19.974, sería la encargada de investigar y recabar todos los antecedentes necesarios para esclarecer los distintos delitos terroristas de la región.

Tal como se dio a conocer posteriormente por la prensa nacional, la labor de la UIOE se centró en recabar múltiples pruebas que vincularan a los entonces ocho sospechosos, con los distintos ataques investigados. Es en este contexto que la Unidad hizo uso del llamado software "Antorcha", el cual de acuerdo con lo señalado por su mismo creador -Alex Smith- permitía interceptar los chats de las aplicaciones WhatsApp, Telegram y Facebook, y, por ende, conocer del contenido de los mensajes intercambiados en estas. El uso de este

[291]Sepúlveda, Nicolas y Arellano, Alberto. (2018) "Operación Huracán": la trama que dinamitó los puentes entre Carabineros y la Fiscalía de Temuco [en línea] Disponible en < https://ciperchile.cl/2018/02/14/operacion-huracan-la-trama-que-dinamito-los-puentes-entre-carabineros-y-la-fiscalia-de-temuco/> [Consultado el 20 de noviembre de 2018]

software solo fue posible en virtud de la Ley N° 19.974, en específico, su artículo 24, el cual, bajo los llamados procedimientos especiales de obtención de información, permite el acceso a canales cerrados de comunicación con el objeto de acceder a ellas y recabar antecedentes necesarios para el cumplimiento de la misión del organismo, dentro de los tantos supuestos que contempla y que previamente fueron analizados.

El 9 de agosto de 2017 el ministro de la Corte de Apelaciones de Temuco, Aner Padilla, en cumplimiento de lo dispuesto en el artículo 25 de la referida ley, otorgó la autorización para el despliegue de las interceptaciones por medio del software. Esto derivó en los hechos previamente mencionados, esto es, la detención de ocho comuneros mapuches, basándose este apremio en los medios probatorios constituidos por las distintas comunicaciones interceptadas por inteligencia.

Sin entrar en mayores detalles referentes al desenvolvimiento posterior del caso, este derivó en un escándalo que significó el cuestionamiento de las pruebas, el cual, desembocó en la comprobación de su falsedad, toda vez que estas habían sido implantadas en los teléfonos celulares de los involucrados.

En cuanto al análisis que importa, primeramente debe atenderse a los mecanismos de control previstos por ley, en relación a medidas tan intrusivas y amplias como las contempladas por la ley. Si bien la necesidad de autorización previa por un ministro de Corte de Apelaciones, y no de un tribunal ordinario, puede significar a simple vista garantía de un control judicial de cierta entidad, no logra ser tal a la luz de los hechos expuestos. La necesidad de esta autorización judicial no importa un análisis exhaustivo de la idoneidad, efectividad y factibilidad de los medios utilizados para desplegar los procedimientos especiales de obtención de información, limitándose estrictamente a la autorización o rechazo de la medida. Es más, la ley no impone estándar alguno tendiente al establecimiento de la motivación del acto de otorgamiento.

El limitado rol que juega el juez en este tipo de casos por mandato legal importa que, en la realidad, tal como ocurrió en este caso, se permita la utilización de herramientas, programas o softwares, entre otros, de a lo menos dudosa procedencia y cuyo real impacto y efectividad solo podrá ser conocido por aquellos que lo utilizan. La circunscripción de su actuación a la mera constatación de la concurrencia de la necesidad de la medida, sin

consideración alguna referente al tipo en específico de procedimiento que se autoriza, solo permite y propicia casos como este. En más, en materias técnicas como estas no debería esperarse que un lego en la materia pueda analizar, someter a juicio y escrutinio este tipo de herramienta, sino que, el mismo legislador debería requerir la intervención de peritos en expertos en la materia. En efecto, como se ha constatado con este caso, la determinación del verdadero funcionamiento de las herramientas autorizadas bajo el articulo 24 escapa de las mismas capacidades y labor que se le ha encomendado a quien se supone debe ejercer la función de control. Esto puede ser consecuencia de su falta de conocimiento técnico, el cual bien puede ser suplido por un perito técnico en la materia, pero a su vez, por la amplitud que otorga la norma en cuestión para utilizar cualquier medio que los servicios de inteligencia estimen.

Esto lleva al segundo punto controvertido a tratar, esto es, la indefinición presente en el artículo 24 de la Ley de Inteligencia, el que en definitiva al no establecer parámetros claros respecto de los procedimientos mismos que han de tomar lugar, permiten un amplio margen discrecional para que los servicios de inteligencias actúen. Esta cuestión se vuelve aún más inquietante si se considera que cualquier herramienta tecnológica que el servicio pretenda utilizar se encuentra permitida por la ley. La única limitante al respecto es el mismo artículo 24, en cuanto es natural que el medio utilizado para desplegar un procedimiento especial de obtención de información sirva efectivamente para esto. Así, las posibilidades son infinitas solo restringidas por la factibilidad técnica, los recursos disponibles, y en definitiva, por la decisión del servicio de inteligencia.

Si bien podría considerarse que dicha libertad es positiva en cuanto permite adaptarse fácilmente a los vertiginosos avances tecnológicos que rigen la actividad de inteligencia, no es menos cierto que esto autoriza un actuar descontrolado y desmedido, posiblemente atentatorio contra los derechos fundamentales de los afectados

Esta indefinición es del todo problemática, en cuanto termina otorgando facultades indeterminadas o irrestrictas a los servicios de inteligencia para acceder a los canales o medios definidos en el artículo 24. Como previamente fue señalado, el mismo TC ha establecido como uno de los requisitos para la determinación de la validez de las

limitaciones a la privacidad, la determinación clara y precisa en forma de habilitaciones restrictas, de las facultades otorgadas al servicio u organismo.

5.3 Decreto Supremo N° 866 de 2017 que establece el Reglamento sobre interceptación de comunicaciones telefónicas y de otras formas de telecomunicación y de conservación de datos comunicacionales.

Las materias reguladas por este decreto pueden ser agrupadas en dos conjuntos, unas destinadas a la determinación de las actividades mismas de vigilancia y otras dedicadas a la regulación de la conservación de datos.

La primera parte en gran medida replica lo establecido en el Decreto 142 de 2005, en cuanto establece una serie de normas las cuales tienen por objetivo el conciliar el resguardo al derecho a la privacidad, con la obtención de información retenida por proveedores de servicios telefónicos en el contexto del desarrollo de una investigación.

Una segunda parte, compuesta por el Titulo III, reglamenta la conservación de las comunicaciones obtenidas por los medios previamente establecidos en los Títulos I y II del Decreto Supremo. Se introducen una serie de modificaciones a lo establecido en la materia por el Código Procesal Penal, en relación a esta materia, así como los organismos que pueden requerirla.

Respecto al primer punto, esto es, la conservación de las comunicaciones, el artículo 80 que esta deberá extenderse por un plazo de a lo menos de dos años, debiendo los prestadores de servicios de comunicaciones deberán conservar todos aquellos datos comprendidos en la definición de comunicación por ese periodo de tiempo o inclusive más.[292]

No tan solo los datos comunicacionales deberán conservarse por este periodo de tiempo, sino que además se requiere que a lo menos estos se acompañen de:

[292] Todo tipo de transmisión, emisión o recepción de signos. señales. Escritos, imágenes, sonidos e información de cualquier naturaleza a los cuales se extiende la interceptación, grabación, observación y monitoreo, que se efectúe por alguno de los medios de telecomunicación establecidos en el artículo 1 de la Ley N° 18.168. tales como comunicaciones, telefónicas, SMM, mms, mensaje a través de diversas aplicaciones de Internet, direcciones IP, URls y/o direcciones de correo electrónico. entre otros.

a) Los antecedentes del suscriptor y/o usuario que permitan conocer los datos administrativos, y financieros de los mismos, sea la forma y medio de pago que utiliza, el período de habilitación y tipo de servicio, entre otros.
b) Los antecedentes necesarios para identificar el origen de la comunicación, tales como número de teléfono. nombre y datos del suscriptor. direcciones IP, entre otros.
c) Los antecedentes necesarios para identificar el destino de la comunicación.
d) Los antecedentes para determinar la fecha, hora y duración de la comunicación.
e) Los antecedentes para determinar la clase o tipo de comunicación.
f) Los antecedentes para determinar los equipos -terminales intervinientes en la comunicación y su ubicación geográfica. con las indicaciones y requisitos que exija la norma técnica respectiva.

Estas disposiciones consideradas en su conjunto se contraponen con lo dispuesto por el Código Procesal Penal, el cual dispone en su artículo 222 que "… los proveedores de tales servicios (prestadores de servicios de comunicaciones) deberán mantener, en carácter reservado, a disposición del Ministerio Publico, 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."

No tan solo se amplía el periodo por el cual los datos han de ser retenidos por los proveedores, por a lo menos el doble del tiempo permitido por el legislador, sino que se impone además la exigencia de acompañar una serie de antecedentes que no son contemplados por el legislador, antecedentes que permiten obtener una extensa cantidad de información respecto del sujeto que ha realizado la comunicación, así como los medios que ha utilizado para realizar esta.

En cuanto a los organismos que pueden requerir dicha información, se debe atender a lo dispuesto en la definición de conservación de datos comunicacionales, los cuales son definidos como "el resguardo y respaldo de los datos a que se refieren las comunicaciones cualquiera sea el medio o forma de telecomunicación, a disposición del Ministerio Público y de toda otra institución que se encuentre facultada por ley para requeridos."

El Decreto Supremo permite que no tan solo al Ministerio Publico en conformidad con lo dispuesto en la norma procesal penal, pueda requerir dicha información, sino que además, a las agencias de inteligencias creadas en la Ley 19.974.

Al regular este Decreto Supremo el ejercicio de derechos fundamentales, como lo son la inviolabilidad de las comunicaciones y el derecho a la privacidad consagrados en el artículo 19 N°4 y N°5 de la CPR, atenta contra el principio básico y general de la reserva legal, el cual rige a nuestro ordenamiento constitucional, ya que tal como lo ha señalado el TC, "en la regulación del ejercicio de los derechos fundamentales; esto es, toca al legislador, y sólo a él, disponer normas al respecto, sin más excepción que la referente al derecho de reunión en lugares de uso público, regido su ejercicio por disposiciones generales de policía, pero tanto aquellas regulaciones como ésta no pueden jamás afectar el contenido esencial de tales derechos".[293]

Un reglamento entendido como una norma de jerarquía inferior a la ley, no puede regular materias referidas al ejercicio de derechos fundamentales, que previamente han sido reguladas por medio de la ley respectiva, en este caso, el Código de Procedimiento Civil. En este mismo orden de ideas, no puede señalarse que el reglamento complementa de forma alguna la ley, toda vez que está ya ha se ha encargado de determinar cuáles son los datos afectos a la conservación y el periodo por el cual esta ha de extenderse, por lo que el reglamento en todo aquello que regula en el caso en cuestión excede su propósito.

Finalmente, en cuanto a los datos que este reglamento permite almacenar, entre los cuales se incluye la geolocalización así como el contenido de la comunicación, permiten llevar a cabo los procesos de agregación e identificación previamente descritos, los cuales permiten aseverar que este reglamento en definitiva permite el desarrollo de la vigilancia masiva a nivel nacional. Las conclusiones que se pueden extraer de los datos, así como el plazo mínimo durante el cual estos deben mantenerse retenidos, permiten entregar a la agencia de inteligencia o al organismo que posea dicha información, un panorama completo de la persona. Se produce una intromisión desmedida en asuntos protegidos por el derecho a la privacidad del sujeto.

[293] Sentencia Tribunal Constitucional de 16 de julio de 1996, rol N°239-96, considerando noveno.

La Contraloría General de la Republica, tomó razón de este Decreto Supremo por medio del Oficio Nº 41.188 del 24 de noviembre del 2017[294], procediendo a su representación. Para esto, utilizó algunos de los argumentos previamente esgrimidos, siendo el de mayor relevancia el referido a las materias tratadas por el Decreto Supremo. A este respecto, tal como se ha señalado, la Contraloría dictaminó qué determinadas disposiciones contenidas en el Decreto debían objetarse en consideración a que estas trataban materias propias de la ley, y que por consiguiente no podían ser reguladas por una disposición de menor jerarquía a la determinada por la Constitución. A este respecto, tanto la regulación de materias concernientes a la conservación de datos comunicacionales por parte de los proveedores de servicios, así como las atribuciones otorgadas a los jueces de garantía y el Ministerio Público, son materias que ya reguladas por la norma correspondiente, en este caso, el Código Procesal Penal, no pueden ser modificadas por un cuerpo normativo de inferior jerarquía.

Otro punto en el cual la Contraloría sustenta la representación dice relación con los términos utilizados en el Decreto Supremo en consideración a la especialidad de la materia tratada por este. En este orden de ideas se declara que determinadas referencias utilizadas, como por ejemplo, "órganos del Estado", o "toda otra institución", son expresiones que no se ajustan debidamente a los preceptos legales regulados por estos. Se presenta un caso de vaguedad en las expresiones utilizadas para regular la materia, que en definitiva permite ampliar a los sujetos u órganos intervinientes en las actividades reguladas por el Decretos Supremo, de forma tal que las facultades extraordinarias otorgadas por este, sean utilizadas de forma generalizadas.

5.4 Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de telecomunicación

A consecuencia de la representación del Decreto Supremo N° 866, continua vigente el Decreto Supremo N° 142 de 2005, el cual se encarga de reglamentar la materia concerniente a la interceptación y grabación de las comunicaciones. El mismo a diferencia

[294] Consultar en <http://www.icdt.cl/wp-content/uploads/2017/11/CGR-representa-decreto-espia.pdf>

del previamente analizado, solo se adentra en determinadas cuestiones técnicas y en la protección de los derechos de los terceros posiblemente afectados por las actividades en el reguladas.

En cuanto a las exigencias técnicas exigidas a las empresas proveedoras de telecomunicaciones, se establece que estas deberán contar con todos los medios necesarios para llevar a cabo las tareas de interceptación como de grabación. A este mismo respecto, ya que las empresas con el propósito de cumplir de este objetivo pueden modernizar sus equipos, el reglamento impone como limite que estos no impidan o dificulten las actividades de interceptación o grabación. Queda de manifiesto cómo ambas exigencias, al no establecer parámetros bajos los cuales, se entenderá el medio utilizado para el desarrollo de la actividad como idóneo, dejan un amplio ámbito discrecional a la autoridad para establecer la cuestión.

En lo que respecta específicamente a la privacidad de los sujetos posiblemente afectados por la actividad, el citado Decreto Supremo les impone a los proveedores la obligación de resguardarla, solo en aquellos casos en que un tercero cuyas comunicaciones se encuentra excluida de la autorización se ve comprometida. Ninguna providencia se establece en este aspecto para resguardar o limitar en lo estrictamente necesario la intervención, en miras de proteger la privacidad del sujeto afectado.

Estas diligencias, en conjunto con las establecidas en el CPP, son realizadas exclusivamente por las fuerzas de seguridad y orden, esto es, Carabineros y la Policía de Investigaciones. Esto no obsta, como se ha señalado, a que particulares mandatos por la ley, en este caso los proveedores de servicios de telecomunicaciones, igualmente estén obligados a realizar este tipo de diligencias, las cuales en su caso en especial solamente se refieren a determinados datos en específicos de sus clientes. A este respecto, la falta de intervención directa por parte Ministerio Público en este tipo de actuaciones se origina en la naturaleza misma del proceso penal que actualmente rige en Chile, producto de la reforma llevada a cabo la década pasada. Así lo manifiesta la misma historia de la ley al señalar que "(…) a afectación de las garantías esenciales de las personas sigue siempre a cargo de la jurisdicción. Es por ello por lo que el ministerio público no puede detener, allanar, interceptar la correspondencia, registrar, etcétera. - En general, no puede adoptar ninguna

conducta que importe vulnerar derechos o garantías constitucionales, sin la previa orden del juez de control de la instrucción."[295]

Finalmente, el Decreto Supremo se encarga de complementar una materia expresamente tratada por el CPP, esto es, la lista de registro de dirección IP de todos sus usuarios. Se produce una discordancia en lo establecido entre ambos cuerpos normativos, toda vez que el CPP señala en el artículo 222, debe comprender un plazo de a lo menos un año de antigüedad, en circunstancias que el Decreto Supremo al referirse al mismo listado determina que este debe remontarse solo en un plazo mínimo de 6 meses. Esta problemática, sin importar las consideraciones que pudieran plantearse en relación a lo gravoso de uno u otro plazo, debe resolverse en favor de lo dispuesto en el CPP, normativa de mayor jerarquía.

CONCLUSIÓN

La innegable expansión a nivel mundial del uso de la vigilancia masiva como herramienta propia de las agencias de inteligencia, nos obliga a plantearnos a nivel nacional cual es el tratamiento que debemos entregarle. Esto importa reconocer que esta no es una actividad pacifica, sino que por el contrario, una que deja en evidencia los peligros a los cuales se exponen los derechos humanos en su constante interacción con la tecnología. En este sentido, el derecho de la privacidad, el cual se erige como uno de los más afectados por esta actividad, exige igualmente el replantear la forma en que es concebido en este escenario.

La inexistencia o falta de conocimiento a nivel nacional del desarrollo de la vigilancia masiva, no puede ser utilizada como una excusa, para a lo menos, iniciar el debate en torno a esta. Nos encontramos inmersos en la era digital, en que la globalización e interconexión son fundamentales. Por lo que su utilización por parte de las agencias de inteligencias nacionales, es a lo menos, inminente.

[295]Historia de la Ley N° 19.696. Primer Trámite Constitucional: Cámara de Diputados Fecha 06 de enero, 1998. Informe de Comisión de Constitución en Sesión 23. Legislatura 336. Informe de la Comisión de Constitución, Legislación y Justicia sobre el Proyecto de Ley que establece un nuevo Código Procesal Penal. Boletín N° 1630-07-1. [en línea] Disponible en < https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/6631/> [Consultado el 19 de noviembre de 2018]

Al plantear las problemáticas que el desarrollo de la vigilancia masiva trae consigo, no debe olvidarse que esta posiciona el centro del debate en la pugna entre seguridad y privacidad. No obstante a que no exista una respuesta unívoca, debe procurarse alcanzar un equilibrio entre ambas, el cual no implique de forma alguna el sacrificio total de una en desmedro de la otra. Alcanzar este balance, importa en último término, resguardar los pilares bajos los cuales una sociedad democrática se cimienta; sin privacidad, o en su defecto sin derechos fundamentales, esta deja de existir. Por esto, se debe tender a encontrar una respuesta que implique la promoción en la mayor medida de lo posible de cada una de estas.

La armonía entre privacidad y seguridad, puede ser alcanzada, como fue descrito en el Capítulo II y III de este trabajo, por medio del establecimiento de pautas claras y objetivas que regulen exhaustivamente el desarrollo de la vigilancia masiva. En efecto, tal como se ha señalado, la experiencia comparada, es aquella a la que Chile debe tender al intentar cualquier aproximación de regulación de esta cuestión. La legislación nacional en materia de inteligencia, así como, de interceptación de las comunicaciones es insuficiente para colmar las exigencias que esta actividad impone. Casos como el de Reino Unido, paradigmáticos en este asunto, exponen los peligros, como los resguardos que deben tomarse al legislar. Una visión omnicomprensiva de las ventajas como de las desventajas de la vigilancia masiva, deben integrar los desarrollos normativos expuestos, así como, los pronunciamientos jurisprudenciales. Estos últimos son de vital importancia toda vez que logran satisfacer las insuficiencias que se han presentado en el primero de estos planos.

Las exigencias que deben cumplirse a este respecto cumplen el amplio espectro desarrollado por el Tribunal Europeo de Derechos Humanos; reconocimiento legal expreso, publicidad de la ley, mecanismos judiciales de control, acceso efectivo a un régimen de recursos, delimitación de los supuestos que la habilitan, duración determinada, notificación posterior de la población afectada, entre otras, son las principales exigencias que deben imponerse.

A pesar de que el desarrollo jurisprudencial logrado ha sido uno de gran relevancia, no debe desconocerse que la vigilancia masiva es una actividad que se encuentra aún en un proceso constante de evolución y perfeccionamiento. Es por esto que debe abogarse por una regulación que además de lo ya mencionado, permita subsanar aquellas deficiencias que en

materia de protección de derechos fundamentales pueda presentarse. No es baladí por consiguiente, el considerar el factor de actualización de la legislación, ya que la tecnología utilizada por la vigilancia masiva lo hace a un ritmo vertiginoso que improbablemente podrá ser alcanzado por la ley.

La implementación del control judicial previo, coetáneo y posterior al desarrollo de esta actividad, no tan solo es necesario en razón de la percepción de peligro respecto de quienes deben llevar a cabo las labores de inteligencia, en cuanto no respeten los límites impuestos, sino que además es primordial esto por la entidad e importancia de los derechos en juego. No son meras expectativas las que se pretenden resguardar por medio de este control, son las garantías bajo las cuales el respeto por la dignidad humana misma se cimienta. Que el control alcance todas las etapas de la vigilancia importa además, el otorgar un resguardo preventivo respecto del despliegue de esta actividad, en cuanto, este permite anticipadamente tutelar los derechos que se ven afectados, y cuya vulneración es imposible reparar. A diferencia de lo que ocurre en sede civil, será imposible una vez que se han vulnerado derechos fundamentales resarcir el daño causado, la indemnización de forma alguna podrá palear o disminuir las vejaciones a las cuales la población se ve expuesta.

El control igualmente debe alcanzar todas las etapas de la vigilancia, esto importa otorgar un resguardo preventivo respecto del despliegue de esta actividad, en cuanto este permite anticipadamente tutelar los derechos que se ven afectados y cuya vulneración es imposible reparar. A diferencia de lo que ocurre en sede civil, será imposible una vez que se han vulnerado derechos fundamentales resarcir el daño causado, y la indemnización de forma alguna podrá palear o disminuir las vejaciones a las cuales la población se ve expuesta.

Urge replantear la forma en que concebimos los derechos humanos, en específico, el derecho a la privacidad en una sociedad altamente tecnológica y vulnerable como la actual. Es un imperativo que a nivel nacional el derecho a la privacidad sea reconocido normativa y jurisprudencialmente no tan solo desde su primitiva concepción, la cual en definitiva solo lo concibe como un espacio de aislamiento respecto de terceros. Se hace necesario introducir a la jurisprudencia nacional los actuales desarrollos doctrinales y jurisprudenciales, que la entienden desde el poder que posee el particular respecto de sus mismos datos. Esto es solo consecuencia de lo ineficaz e irreal que resulta no entender el

derecho a la privacidad desde a lo menos una perspectiva de control respecto de los datos e información de propiedad de un sujeto, lo cual es esencial en su consideración en relación a la tecnología y los nuevos medios de comunicación los cuales permiten aumentar exponencialmente la vulnerabilidad de este derecho.

La intrínseca vinculación de la privacidad con la tecnología, conlleva el establecer un nuevo límite de lo que se considerada resguardado por este derecho. Su ámbito de protección se ha restringido en cuando la información disponible a consecuencia del actuar de las mismas personas ha aumentado. La delimitación de lo tutelado por la privacidad, por consiguiente, debería a lo menos abarcar aquel contenido no expuesto en plataformas digitales, y todo aquello que a pesar de encontrarse comprendido dentro de estas, y otros aparatos digitales, no es objeto de divulgación consentida.

Además, la privacidad en el derecho chileno al hacer suyo este tipo de avances tecnológicos, debe a los menos jurisprudencialmente innovar en la determinación de los criterios que tradicionalmente se han impuesto para permitir la limitación de la privacidad. No se trata de que ahora en más deban estos deban ser abandonados; por el contrario, sobre su base se deben construir y adaptar los nuevos criterios en función de la vigilancia masiva u otro tipo de actividades de inteligencia. La proscripción de habilitaciones irrestrictas por ejemplo, al exigir la delimitación específica y clara de las facultades entregadas,

Esta determinación, aun cuando en el caso de adoptarse en la realidad sea distinta, siempre deberá a lo menos considerar las expectativas básicas de reserva sobre las cuales el derecho a la privacidad se ha construido. Esto importa concluir que, pese a que cierta información o datos sean de fácil acceso, estos no pueden ser considerados por este solo hecho como abiertos y de acceso general. De no existir un conocimiento real por parte de las personas de su uso, estos no podrán ser utilizados.

BIBLIOGRAFIA

1. Alto Comisionado de las Naciones Unidas para los Derechos Humanos, El derecho a la privacidad en la era digital, 2014. [en línea] Disponible en <http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_28_L27.pdf> [Consultado el 1 de abril de 2018]

2. Ayala Corao, Carlos M. (2000). El Derecho Humano a la Libertad de Expresión: Limites aceptados y responsabilidades ulteriores. Ius et Praxis [en línea] Disponible en:<http://www.redalyc.org/articulo.oa?id=19760106> [Consultado el 22 de septiembre de 2018]

3. Banda Vergara, Alfonso. (2000) Manejo de Datos Personales un Límite al Derecho a la Vida Privada Revista de Derecho (Valdivia), vol.11, p.55-70.

4. Bárcena Cochi, Martha. (2000) La reconceptualización de la seguridad: El Debate Contemporáneo [en línea] Disponible en <https://revistadigital.sre.gob.mx/images/stories/numeros/n59/barcena.pdf> [Consultado el 12 de abril de 2018.]

5. Barinas Ubiña, Désirée. 2013. El Impacto de las Tecnologías de la Información y de la Comunicación en el Derecho a la Vida Privada: Las Nuevas Formas de Ataque a la Vida Privada. Revista Electrónica de Ciencia Penal y Criminología. [en línea] N° 15 Disponible en < https://dialnet.unirioja.es/servlet/articulo?codigo=4407594 > [Consultado el 15 de junio de 2018]

6. Barros Bourie, Enrique. (1998) Honra, privacidad e información: un crucial conflicto de bienes jurídicos Revista de Derecho Universidad Católica del Norte, N°5, pp. 45-58.

7. Bigo, D, Carrera, S, Hernanz, N, Jeandesboz, J.A, Parkin, J, Ragazzi, F y Scherrer, A. (2013) National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law. [en línea] Disponible en < https://dare.uva.nl/search?identifier=95882891-5efc-4211-b502-6da9080e9509> [Consultado el 24 de abril del 2018]

8. Borges, Bruno y Santoro, Mauricio. (2016) Brazilian Foreign Policy Towards Internet Governance. [en línea] Disponible en <http://www.scielo.br/pdf/rbpi/v60n1/1983-3121-rbpi-60-01-e003.pdf> [Consultado el 2 de junio de 2018]

9. Botero, Catalina Libertad de Expresión e Internet. (2013) Relatoría Especial para la Libertad de Expresión Comisión Interamericana de Derechos Humanos. [en línea] Disponible en <http://pensamientocivil.com.ar/system/files/2014/07/Miscelaneas115.pdf.> [Consultado el 24 de septiembre de 2018]Apéndice 2°

10. Cea Egaña, José Luis, (2000). Los Derechos a la Intimidad y a la Honra en Chile. Ius et Praxis. [en línea] Disponible en <http://www.redalyc.org/articulo.oa?id=19760208> ISSN 0717-2877 [Consultado el 21 de septiembre de 2018].

11. Cinta Caminals Jordi, Jové. () Las Reformas del Código Penal 2015. [en línea] Disponible en <https://app.vlex.com/#WW/search/jurisdiction:ES+content_type:4/interceptación/vid/573859007> [Consultado el 21 de noviembre de 2018]

12. Consultar los archivos desclasificados por la Agencia Nacional de Seguridad de Estados Unidos de Norteamérica en < https://www.nsa.gov/news-features/declassified-documents/ukusa/>

13. Corral Talciani, Hernán. (2000) Configuración Jurídica del derecho a la privacidad, Revista Chilena de Derecho, Vol. 27 N°2.

14. Corral Talciani, Hernán. (2000) Configuración Jurídica del Derecho a la Privacidad II: Concepto y Delimitación. Revista Chilena de Derecho, Vol. 27 N°2

15. Corte Interamericana de Derechos Humanos, Molina Theissen Vs. Guatemala. Fondo. Sentencia de 4 de mayo de 2004. Serie C No. 106

16. Council of Europe, Mass Surveillance. (2017). [en línea] Disponible en <https://rm.coe.int/factsheet-on-mass-surveillance-corrected-and-final-

rev2august2017/1680736031Thematic factsheet1> [Consultado el 20 de septiembre de 2018]

17. Cross, Jennifer. Cybersecurity and the rights of the internet user in France. [en línea]Disponible en <http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=2400&context=gjicl.>

18. D. Cohen, Elliot. (2014). Technology of oppression: Preserving Freedom and Dignity in Age of Warrantless Mass Surveillance. New York, Palgrave MacMillan.

19. D. Velásquez, Juan y Donoso, Lorena. (2009). Web Mining: Análisis sobre la Privacidad del Tratamiento de Datos Originados en la Web. [en línea] Revista Ingeniera de Sistemas. Volumen XXIII, septiembre 2009. Disponible en < http://www.dii.uchile.cl/~ris/RISXXIII/Velasquez5.pdf > [Consultado el 20 de mayo 2018]

20. Fernández Segado, Francisco (1990) La libertad de expresión en la doctrina del Tribunal Europeo de Derechos Humano. [en línea] Disponible en <http://roderic.uv.es/handle/10550/47836> [Consultado el 20 de abril de 2018]p. 95

21. Fuentes Cubillos, Hernán. (2008). El principio de proporcionalidad en el Derecho Penal. Algunas consideraciones acerca de su concretización en el ámbito de la individualización de la pena. [en línea] Ius et Praxis v.14 n.2 Talca**.** Disponible en https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-00122008000200002> [Consultado el 28 de septiembre de 2018]

22. Galván, Ezequiel Rodrigo (2016) Libertad de expresión e Internet. [en línea] Disponible en <http://sedici.unlp.edu.ar/bitstream/handle/10915/58287/Documento_completo.pdf-zDFA.pdf?sequence=1&isAllowed=y> [Consultado el 22 de septiembre de 2018]

23. Gandulo R., Eduardo. (1999) Principios de Derecho Procesal en el Nuevo Sistema de Procedimiento. Revista de Derecho de la Universidad Católica de Valparaíso XX Valparaíso, Chile.

24. García Ramírez, Sergio y Gonza, Alejandra. (2007). Jurisprudencia de la Corte Interamericana de Derechos Humanos. [en línea] Disponible en <http://anaforas.fic.edu.uy/jspui/bitstream/123456789/25380/1/libertad-expresion.pdf.> [Consultado el 20 de septiembre de 2018]

25. Garriga Domínguez, Ana. (2016). Nuevos retos para la Protección de Datos Personales. En la Era del Big Data y la Información Oblicua. [en línea], Madrid, Dykinson. Disponible en <https://app.vlex.com/#WW/sources/14328> [Consultado el 30 de marzo].

26. Geist, Michael. (2015) Law, Privacy and Surveillance in Canada in the Post-Snowden Era. [en línea] Disponible en <https://press.uottawa.ca/law-privacy-and-surveillance.html> [Consultado el 2 de junio de 2018]

27. González San Juan, José Luis. (2015) Jurisprudencia española sobre la protección del honor, la intimidad y la propia imagen en Internet. [en línea] Disponible en < https://www.ibersid.eu/ojs/index.php/ibersid/article/viewFile/4215/3825 > [Consultado el 10 de noviembre de 2018] p.84

28. Handbook on European Data Protection Law. [en línea] Disponible en <https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdfz > Consultado el 1 de octubre de 2018]

29. Historia de la Ley N° 19.696. Primer Trámite Constitucional: Cámara de Diputados Fecha 06 de enero, 1998. Informe de Comisión de Constitución en Sesión 23. Legislatura 336. Informe de la Comisión de Constitución, Legislación y Justicia sobre el Proyecto de Ley que establece un nuevo Código Procesal Penal. Boletín N° 1630-07-1. [en línea] Disponible en < https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/6631/> [Consultado el 19 de noviembre de 2018]

30. Informe Anual sobre Derechos Humanos en Chile 2017 (en línea). Santiago de Chile, Universidad Diego Portales, 2017. p. 395. Disponible en <http://www.derechoshumanos.udp.cl/derechoshumanos/index.php/informe-anual> [Consultado el 1 de abril de 2018]

31. Informe Sobre la Existencia de un Sistema Mundial de Interceptación de Comunicaciones Privadas y Económicas, de 11 de junio de 2001 [en línea] Disponible en <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//ES> [Consultado el 17 de abril del 2018]

32. Ivelic Mancilla, Alejandro. (2014) Las Interceptaciones de Comunicaciones Telefónicas en los Delitos de Tráfico Ilícito de Estupefacientes. Revista Jurídica del Ministerio Público, N° 60.

33. J. Solove, Daniel. (2008). Understanding Privacy, Harvard University Press. GWU Legal Studies Research Paper N° 420.

34. López-Barajas Perea, Inmaculada (2016) Aplicación de las Tecnologías de la Información y de la Comunicación a la Investigación Criminal: la Reforma de la Ley de Enjuiciamiento Criminal Española de 2015 [en línea] Revista Iberoamérica de Sistemas, Cibernética, e Informática Volumen 13 N° 2, Año 2016. Disponible en < http://www.iiisci.org/journal/risci/FullText.asp?var=&id=CA489BC16> [Consultado el 25 de noviembre de 2018] 17

35. López-Barajas Perea. (2017) Inmaculada, Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos. IDP. Revista de Internet, Derecho y Política [en línea] Revista de los Estudios de Derecho y Ciencia Política Disponible en <http://www.redalyc.org/html/788/78850913006/> [Consultado el 26 de noviembre de 2018

36. Marco Civil Brasileño de Internet, (2015), Centro de Documentación e Información Edições Câmara Brasília. [en línea] Disponible en <https://eva.fing.edu.uy/pluginfile.php/99128/mod_resource/content/1/marco_%20civil%20_internet.pdf> [Consultado el 1 de Octubre de 2018]

37. Martínez de Pisón Cavero, José. (1994) La Constitucionalidad del derecho a la Intimidad. [en línea]Derechos y Libertades: revista del Instituto Bartolomé de las Casas. ISSN: 1133-0937. II (3). p. 313—340. Disponible en <https://docs.google.com/viewerng/viewer?url=https://e-

archivo.uc3m.es/bitstream/handle/10016/1493/DL-1994-II-3-Pison.pdf> [Consultado el 12 de noviembre de 2018]

38. Martínez de Pisón, José. (2016) El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional. [en línea] Anuario de Filosofía del Derecho, N° 32 págs. 409-430. Disponible en < https://dialnet.unirioja.es/servlet/articulo?codigo=5712518 > [Consultado el 22 de noviembre de 2018]

39. Martínez de Pisón, José. (2016) Vida Privada sin Intimidad. Una Aproximación a los Efectos de las Intromisiones Tecnológicas en el Ámbito Intimo. [en línea] Disponible en <https://www.researchgate.net/publication/320901364_Vida_privada_sin_intimidad_Una_aproximacion_a_los_efectos_de_las_intromisiones_tecnologicas_en_el_ambito_intimo > [Consultado el 2 de noviembre de 2018].

40. Naciones Unidas, Asamblea General. Resumen de la mesa redonda del Consejo de Derechos Humanos sobre el derecho a la privacidad en la era digital (2016) A/HRC/2839. [en línea] Disponible en < http://webcache.googleusercontent.com/search?q=cache:DL-7zW4tkdgJ:docstore.ohchr.org/SelfServices/FilesHandler.ashx%3Fenc%3DdtYoAzPhJ4NMy4Lu1TOebIM8c1X4GZjGEGHV9SBM9XSLrkyhn8X9OP5PErl472DFS0WGHKjiDqlMTqWwtmsbg%252B0%252FwzDfM6vlTrrWIR7iAZGazm7af2xJyOwQ13wo5CrT+&cd=1&hl=es&ct=clnk&gl=cl>. [Consultado el 26 de noviembre de 2018]

41. Navarro, B.H Y Carmona, S. C. (2005) Recopilación de Jurisprudencia del Tribunal Constitucional (1981-2005). Cuadernos del Tribunal Constitucional. N° 59. p.190.

42. Nieves Saldaña, María. (2011) El derecho a la privacidad en los Estados Unidos: Una aproximación diacrónica a los intereses constitucionales en juego. [en línea] Disponible en <http://revistas.uned.es/index.php/TRC/article/view/6960> [Consultado el 25 de mayo de 2018]

43. Nogueira Alcalá, Humberto. (1998). El Derecho a la Privacidad y a la Intimidad en el Ordenamiento Jurídico Chileno. [en línea] Ius et Praxis. Disponible

en:<http://www.redalyc.org/articulo.oa?id=19740206> [Consultado el 29 de julio de 2018]

44. Olezza, Marina Florencia (2017) Aspectos Epistemológicos de la Infoesfera Revista Perspectivas Metodológicas /19/Vol. II.

45. Organización de las Naciones Unidas, Asamblea General. "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue" Resolución A/HRC23/40, [en línea] Disponible en <https://undocs.org/es/A/HRC/23/40> [Consultado el 26 de noviembre de 18]

46. Organización para Cooperación y desarrollo Económico, Directrices de la OCDE que regulan la protección de la privacidad y el flujo fronterizo de datos personales, 1981, [en línea] Disponible en <http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf> [Consultado el 1 de abril del 2018] p.22

47. Parlamento Europeo, Informe sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE. UU, los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos de Interior, 21 de febrero de 2014. [en línea] Disponible en <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//ES#title2> [Consultado el 17 de abril de 2018]

48. Parsons, Christopher, Lex Gill, Tamir Israel, Bill Robinson, y Ronald Deibert. (2007) Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act respecting national security matters), University of Toronto. [en línea], Disponible en <https://citizenlab.ca/wp-content/uploads/2017/12/C-59-Analysis-1.0.pdf> [Consultado el 2 de octubre de 2018]

49. Pérez Luño, Antonio. (2002) Internet y los Derechos Humanos Anuario de Derechos Humanos. Nueva Época. Vol. 2, págs. 101-121.

50. Pérez Luño, Antonio-Enrique. (1981) Informática y Libertad. Comentario al Artículo 18.4 de la Constitución Española. Revista de Estudios Políticos (Nueva Época) Núm. 24, Noviembre -Diciembre 1981.

51. Petición realizada por ASSOCIATION CONFRATERNELLE DE LA PRESSE JUDICIARE and 11 otras asociaciones v. Francia. <https://privacyinternational.org/sites/default/files/2018-09/2017.09.15%20PI%20French%20Surveillance%20Intervention.pdf> p. 2

52. Pfeiffer, María Luisa. (2008). Derecho a la privacidad. Protección de los datos sensibles. Revista Colombiana de Bioética [en línea], 3 (Enero-Junio) Disponible en: <http://www.redalyc.org/articulo.oa?id=189217248002> [Consultado el 20 de noviembre de 2018]

53. Podkowic, Jan. (2015) Vigilancia y privilegio periodístico en la era de las nuevas tecnologías de las telecomunicaciones bajo la Convención de Derechos Humanos y Libertades Fundamentales y la Constitución de la República de Polonia. [en línea] Disponible en <https://dialnet.unirioja.es/servlet/articulo?codigo=5265507> [Consultado el 24 de septiembre de 2018]

54. Principios Tshwane [en línea] Disponible en < https://www.opensocietyfoundations.org/sites/default/files/tshwane-espanol-10302014%20%281%29.pdf> [Consultado el 20 de septiembre de 2018]

55. Puerto, María Isabel y Sferrazza-Taibi, Pietro. (2018) La sentencia Schrems del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional. Revista Derecho Estado n.40 [en línea]. Disponible en < http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S0122-98932018000100209&lng=en&nrm=iso > [Consultado el 25 de noviembre de 2018]

56. Quezada Rodríguez, F. (2014). La protección de datos personales en la jurisprudencia del Tribunal Constitucional. Revista de Derecho Público, (76), Págs. 425-441

57. Rackow Sharon H (2002) How the USA Patriot Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of "Intelligence"

Investigations [en línea] Disponible en <https://www-jstor-org.uchile.idm.oclc.org/stable/pdf/3312949.pdf> [Consultado el 1 de junio de 2018]

58. Rayman Labrín, Danny. (2015). Chile: Vigilancia y el derecho a la privacidad en internet. Revista Chilena de Derecho y Tecnología, Chile, Vol. 4 (1): 206, 2015.

59. Relatoría para la Libertad de Expresión Comunicado de Prensa, R 50/15 [en línea] Disponible en <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=990&lID=2> [Consultado el 26 de septiembre de 2018]

60. Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court JANUARY 23. (2014) [en línea] Disponible en https://www.justsecurity.org/wp-content/uploads/2014/01/Final-Report-1-23-14.pdf, [Consultado el 30 de septiembre de 2018]. p. 22

61. Sanjurjo Ríos, Eva Isabel. (2017) Las Conversaciones de WhatsApp como objeto de Investigación y Prueba en el Proceso Penal [en línea] Justicia: Revista de Derecho Procesal. N°1/2017. Disponible en < https://app.vlex.com/#WW/search/jurisdiction:ES+content_type:4/interceptaci%C3%B3n/vid/703952709> [Consultado el 21 de noviembre de 2018]

62. Sentencia del Tribunal Constitucional del 30 de octubre de 1995, rol 226-95, considerando noveno.

63. Sentencia Tribunal Constitucional de 11 de septiembre de 2012, rol N° 2153-11-INA, considerando trigésimo primero.

64. Sentencia Tribunal Constitucional de 12 de julio de 2012, rol N°1894-2011, considerando vigésimo primero.

65. Sentencia Tribunal Constitucional de 12 de julio de 2012, rol Nº 1894-2011, considerando vigésimo primero.

66. Sentencia Tribunal Constitucional de 16 de julio de 1996, rol N°239-96.

67. Sentencia Tribunal Constitucional de 20 de abril de 2004, rol N°1273, considerando cuadragésimo segundo.

68. Sentencia Tribunal Constitucional de 25 de noviembre de 2014, rol N° 2731-14.

69. Sentencia Tribunal Constitucional de 28 de octubre de 2010, rol N ° 389-03, considerando vigésimo segundo.

70. Sentencia Tribunal Constitucional de 28 de octubre de 2013, rol N° 389-2013, considerando vigésimo quinto.

71. Sentencia Tribunal Constitucional de 31 de enero de 2013, Rol N° 2246-2012, considerando trigésimo cuarto.

72. Sentencia Tribunal Constitucional de 31 de enero de 2013, rol N°2246-2012, considerando trigésimo cuarto.

73. Sentencia Tribunal Constitucional de 31de enero de 2013, rol N°2246-2014, considerando quincuagésimo sexto.

74. Sentencia Tribunal Constitucional de 5 de junio de 2012, rol N°1990-11, considerando vigésimo tercero.

75. Sentencia Tribunal Constitucional de 5 de junio de 2012, rol N°1990-11, considerando trigésimo segundo.

76. Sentencia Tribunal Constitucional de 8 de abril de 2010, rol N° 1365-09-INA, considerando trigésimo séptimo.

77. Sentencia Tribunal Constitucional del 10 de octubre de 2003, rol N° 389-2003, considerando vigésimo primero.

78. Sentencia Tribunal Constitucional del 28 de octubre de 2003, rol N° 389, considerando décimo séptimo.

79. Solove J, Daniel. (2006). A taxonomy of privacy. [en línea]. Disponible en <p.490https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477.pdf> [Consultado el 18 de junio de 2018]

80. Solove, Daniel J. (2007). "I've got nothing to hide and other Misunderstanding of Privacy, [en línea]. Disponible en <https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1159&context=faculty_publications> Consultado el 25 de septiembre.

81. Solove, Daniel J. (2008). Data mining and the Security-Liberty debate. [en línea] Disponible en < https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=5659&context=uclrev> [Consultado el 25 de septiembre de 2018]

82. Solove, Daniel J. (2011). Nothing to hide: The false Tradeoff Between Privacy and Security. Yale University Press.

83. Suarez, Sergio (2017) Is America Safer? The USA FREEDOM Act of 2015 and What the FBI and NSA Have, Can, and Should be Doing. [en línea] Disponible en <https://scholarship.shu.edu/cgi/viewcontent.cgi?referer=https://www.google.cl/&httpsredir=1&article=1888&context=student_scholarship> [Consultado el 30 de septiembre de 2018]

84. The Guardian. Edward Snowden and the NSA-time files [en línea] Disponible en <https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline> [Consultado el 26 de noviembre de 2018]

85. Tribunal Constitucional de 12 de Julio de 2011, rol N° 1894-2011, considerando vigésimo primero.

86. Tribunal Constitucional de 9 de mayo del 2016, rol N° 3016(3026)-16-CPT, voto por acoger, considerando séptimo.

87. Tribunal Constitucional español en la STC 254/1993, fojas.6.

88. Tribunal Constitucional Español Sentencia 121-2002 de 20 de mayo de 2002 Fundamento 2°

89. Tribunal Constitucional español, de 7 de noviembre N° 173/2011

90. Tribunal Constitucional español, Rol N° 2246-2012, 31 de enero de 2013

91. Tribunal de Justicia de la Unión Europea, C-293/12. Digital Rights Ireland y Seitlinger y Otros. Sentencia de 8 de abril de 2014

92. Tribunal de Justicia de la Unión Europea, caso Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros C-293/12, de 8 de abril de 2014.

93. Tribunal de Justicia de la Unión Europea, caso Maximillian Schrems y Data Protection Commissioner v. Facebook Ireland Limitada. C-498/16, 6 de octubre de 2015.

94. Tribunal Europeo de Derechos Humanos Caso Tillack v. Belgica. Solicitud 20477/05, del 27 de noviembre de 2007.

95. Tribunal Europeo de Derechos Humanos, Caso Weber v. Saravia N°54934/00.

96. Tribunal Europeo de Derechos Humanos. Caso Big Brother Watch y otros v. El Reino Unido. N° 58170/13

97. Tribunal Europeo de Derechos Humanos. Caso Klass y otros. v. Alemania, N° 15473/1989.

98. Tribunal Europeo de Derechos Humanos. Caso Leander y Segerstedt v. Suiza. N° 9248/81.

99. Tribunal Europeo de Derechos Humanos. Caso Liberty y otros v. Reino Unido. N° 58243/00.

100. Tribunal Europeo de Derechos Humanos. Caso Olsson v. Suecia. N° 74/1991/326/398.

101. Tribunal Europeo de Derechos Humanos. Caso Zhakarov v. Rusia. N° 47436/06. Apéndice 180

102. Tribunal Europeo de Derechos Humanos.Caso Shmolov v. Rusia. N° 30194/09. Apéndice 68

103. Vazán, Victor. (2005). El Habeas Data y el Derecho de Autodeterminación Informativa en Perspectiva de Derecho Comparado. [en línea] Estudios Constitucionales, vol. 3, núm. 2, pp. 85-139. Disponible en

<https://app.vlex.com/#CL/search/jurisdiction:CL/autodeterminacion+informativa/CL/vid/43011320> [Consultado el 17 de abril del 2018]

104. Vidal Prado, Carlos. (2017). La libertad de Expresión en la Jurisprudencia del Tribunal Constitucional Federal Alemán. Estudios Constitucionales Año 15, N ° 2, 2017, pp. 273-300 [en línea] Disponible en:<http://www.redalyc.org/articulo.oa?id=82054982008> [Consultado el 2 de octubre de 2018]

105. Weezel van, Alex - Darricades, (2011) Tomás, Interceptaciones telefónicas. Oportunidad para avanzar, en Revista del Abogado del Colegio de Abogados de Chile, 52, (julio de 2011), pp. 40-43.

106. Whitaker, Reg. (1999) El fin de la privacidad: Cómo la vigilancia total se está convirtiendo en realidad. The New Press, Nueva York.

107. Whitehead W., John y. Aden Steven. (2002) Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA Patriot Act and the Justice Department's AntiTerrorism Initiatives. [en línea] Disponible en <http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1149&context=aulr> [Consultado el 1 de junio de 2018]