REVISTA CHILENA DE DERECHO Y TECNOLOGÍA
CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO • UNIVERSIDAD DE CHILE
ISSN 0719-2576 • VOL. 4 NÚM. 1 (2015) • PÁGS. 187-232 • DOI 10.5354/0719-2584.2015.36007

Chile: Vigilancia y derecho a la privacidad en internet

Chile: Surveillance and the right to privacy on internet

DANNY RAYMAN LABRÍN
Abogado, Juan Pablo González & Compañía Abogados, Chile

RESUMEN El presente artículo estudia la relación entre la vigilancia en internet y la afectación del derecho a la privacidad en Chile. Específicamente se centra en el uso de este tipo de vigilancia por parte del Estado con el fin de cumplir objetivos legítimos, como la prevención del delito y la protección de la seguridad de sus habitantes. Con dicho motivo el autor analiza las normas de intromisión a la privacidad que se vinculan con la vigilancia en internet, lo señalado por el Alto Comisionado de las Naciones Unidas para los Derechos Humanos al respecto y dos antecedentes que tienen origen en Chile, a saber, el caso del alumno universitario Bryan Segel y un reportaje realizado a funcionarios de las policías de Chile. El estudio de estos antecedentes en su conjunto permiten concluir, por una parte, que las medidas de vigilancia en internet son arbitrarias e ilegales en Chile, debido a que no cumplen con los principios de legalidad, necesidad y proporcionalidad; y, por otra parte, que Chile al adoptar este tipo de intromisiones a la privacidad incumple con sus obligaciones internacionales en materia de derechos humanos al no respetar dichos principios.

PALABRAS CLAVE Derechos fundamentales, derechos humanos, dere-

cho a la privacidad, derecho a la libertad de expresión, internet, metadatos, vigilancia.

ABSTRACT This article studies the relationship between the infringement of the right to privacy and Internet surveillance in Chile. Specifically it is focusing on the use of such surveillance by the State in order to fulfill legitimate objectives such as crime prevention and the protection of the safety of its inhabitants. At that occasion the author analyzes the rules of interference to privacy that are linked to surveillance on the Internet, the stated by the Office of the United Nations High Commissioner for Human Rights related to it, and two antecedents originate in Chile, namely, the case of the college student Bryan Segel and a report made to police officers of Chile. The study of these backgrounds together enable him to conclude, firstly, that surveillance measures on the Internet are arbitrary and illegal in Chile, because they do not comply with the principles of legality, necessity and proportionality; and moreover that Chile in adopt this type of interferences to privacy breach of its international obligations on human rights by failing to respect these principles.

KEYWORDS Fundamental rights, human rights, right to privacy, right to freedom of speech, Internet, metadata, surveillance.

INTRODUCCIÓN

En los últimos años internet se ha vuelto una herramienta imprescindible no sólo para el desarrollo de nuevos modelos de negocios, sino también como una herramienta social y democratizadora que ha dado fuerza a diversas manifestaciones sociales y culturales desde el «ciberespacio» al mundo real. Ejemplos paradigmáticos de ello son la revolución egipcia, Ocuppy Wall Street, el movimiento de los indignados en España, las recientes manifestaciones por racismo en Ferguson, Estados Unidos, entre otros. Todos, en alguna medida, se potenciaron gracias a la web y, de seguro, sin ella su impacto no hubiera sido el mismo.

Esto es posible porque internet constituye un espacio libre, donde sus usuarios se mueven sin mayores restricciones, pudiendo manifestarse tanto sobre temas políticos como sobre temas personales. De esta forma, internet es principalmente una plataforma para la libertad de expresión.

Pese a lo anterior, la libertad en internet no está exenta de restricciones. En reiteradas oportunidades hemos visto cómo diversas iniciativas han intentado limitar la información que circula, como ocurrió a principios del año 2014 en Turquía, donde se bloqueó Twitter gracias a una ley que facilitó a las autoridades cerrar sitios web y acceder a información personal de los usuarios, sin orden judicial.[1]

Pero no es sólo el control de la información lo que genera problemas, sino también la vigilancia a la que estaríamos sujetos los usuarios de internet, situación que quedó al descubierto luego de las revelaciones realizadas por Edward Snowden durante el año 2013, haciendo públicos documentos clasificados sobre los programas de vigilancia masiva del gobierno de Estados Unidos, donde incluso participaron algunas de las compañías tecnológicas más importantes, como Facebook, Google, Microsoft, entre otras.

De esta forma, la vigilancia en internet se caracteriza por: i) dirigirse a grandes grupos de usuarios de internet; ii) recopilar, almacenar y analizar la información que los mismos usuarios de internet generan y suben a la web; iii) determinar los actos, conductas, preferencias, localización y otras características que permiten individualizar a cada usuario de internet junto con aspectos de la vida privada que nunca tuvieron la intención de revelar. Debido a estas características es que la vigilancia en internet representa un gran peligro para los derechos fundamentales de las personas.

En este trabajo analizaremos la legitimidad de la aplicación de este tipo de medidas por parte del Estado, entendiendo que la vigilancia en internet es empleada por Chile con finalidades como el resguardo del orden, la prevención del delito y la protección de su propia seguridad.

Es posible constatar que en el último tiempo en Chile se han llevado a cabo medidas de vigilancia en internet por parte de las autoridades. Por

1. Véase «Turquía bloquea Twitter y amenaza a otras redes sociales», *FayerWayer*, 21 de marzo de 2014, disponible en <http://bit.ly/1Cpt9Ln> y «Turquía aprueba leyes extremas para controlar Internet», *FayerWayer*, 6 de febrero de 2014, disponible en <http://bit.ly/1NTHlxy>. Cabe señalar que Turquía tiene en su historial otras conductas similares, como por ejemplo el bloqueo que hizo a Youtube. Véase «Youtube vuelve a ser accesible en Turquía», *FayerWayer*, 31 de octubre de 2010, disponible en <http://bit.ly/1UBHFpp> y «Turquía vuelve a censurar Youtube», *FayerWayer*, 3 de noviembre de 2010, disponible en <http://bit.ly/1LSHHoV>.

ejemplo, un reportaje del año pasado reveló prácticas de la Policía de Investigaciones y del Ministerio Público a la hora de recopilar información respecto de personas bajo investigación o sospecha;[2] y un estudiante de sociología fue formalizado por haber cometido maltrato de obra en contra de un teniente de Carabineros de Chile, teniendo como principal medio de prueba incriminatorio la información obtenida desde las redes sociales.[3]

De esos antecedentes, se podría sostener que el Estado de Chile afecta el derecho a la privacidad al no cumplir con los principios de legalidad, necesidad y proporcionalidad, afectando a su vez otras garantías constitucionales, entre ellas la libertad de expresión, razón por la que a su vez Chile incumple con sus obligaciones internacionales en materia de derechos humanos.

Para fundamentar esta conclusión, nos referiremos en primer lugar al derecho a la privacidad en internet. Luego, en un segundo punto, nos referiremos a la vigilancia en internet con el objeto de definirla, para posteriormente examinar los tipos de intromisión a la privacidad en internet que contempla el ordenamiento jurídico de Chile y que se relacionan con la vigilancia.

Señalado lo anterior, será necesario preguntarse si el ordenamiento jurídico nacional contempla y faculta a las autoridades a implementar la vigilancia en internet. Para responder esta pregunta analizaremos lo señalado por el Alto Comisionado de Naciones Unidas para los Derechos Humanos y, a su vez, los hechos y el contexto de los dos casos señalados precedentemente. Lo anterior nos permitirá reflexionar en torno al cumplimiento o no de los principios requeridos para considerar si nos encontramos ante injerencias legales o bien ilegales y/o arbitrarias cuando el Estado de Chile, en la búsqueda de objetivos legítimos, utiliza la vigilancia en internet.

---

2. «Trabajo policial usa cada vez más los datos de *Facebook* para atrapar delincuentes», *La Segunda*, 16 de junio de 2014, disponible en <http://bit.ly/1eH6vmT>.

3. Sentencia Séptimo Juzgado de Garantía de Santiago de fecha 20 de mayo de 2014, rol interno O-8316-2014. Por su parte es posible ver las siguientes noticias al respecto: «Sospechoso de ataque a carabinero queda en libertad», *24 Horas*, 20 de mayo de 2014, disponible en <http://bit.ly/1JUCw5K>, y «Defensa de estudiante formalizado por ataque a teniente evalúa reclamo en Fiscalía», *BioBio Chile*, 20 de mayo de 2014, disponible en <http://bit.ly/1Hgzgk2>.

DERECHO A LA PRIVACIDAD EN INTERNET

ORÍGENES DEL DERECHO A LA PRIVACIDAD

Muchas veces, al hablar de los inicios del derecho a la privacidad, tendemos a pensar en los abogados estadounidenses Samuel Warren y Louis Brandeis, quienes en el año 1890 publicaron el artículo «The Rigth to Privacy» el cual dio forma a la tradicional definición de privacidad (Warren y Brandeis, 1995). Sin embargo, el reconocimiento de este derecho viene desde hace siglos atrás.

La privacidad como derecho está profundamente arraigado en la historia de la humanidad. Pese a que durante siglos no existió una referencia directa que conceptualizara o definiera este derecho, sí existieron múltiples referencias a él, incluso desde la época antigua, tal como dan cuenta el Corán y la Biblia.[4] Por su parte en Inglaterra, en el año 1361, la Ley de Jueces de Paz permitió el arresto de mirones y fisgones (cf. Michael, 1994). Siglos después, el reconocimiento de la importancia de la privacidad se siguió consolidando gracias a los aportes de Lord Camden[5] y el parlamentario William Pitt.[6] En el caso de Suecia, en el año 1776 se pro-

4. The Electronic Privacy Information Centre y Privacy International, en su informe denominado *Privacidad y derechos humanos*, se refiere a los orígenes de la privacidad señalándonos que su reconocimiento se puede hallar en textos milenarios como en el Corán y en los proverbios de Mahoma, así como también en la Biblia. Esta última cuenta con numerosas referencias a la privacidad. Por su parte, nos señalan que en la ley judía se reconoció por mucho tiempo el concepto de estar libre de la mirada de los demás. Incluso hacen referencia a protecciones que habrían existido en la Grecia clásica y en la antigua China (Cedric Laurant, 2012: 19).

5. En el año 1765 Lord Camden anuló una orden judicial de registro de domicilio y confiscación de documentos haciendo una referencia directa a la importancia de los documentos privados, señalando que «podemos decir con seguridad que no existe ley en este país para justificar a los acusados por lo que hicieron; si la hubiera, ésta destruiría todo el bienestar de la sociedad, pues los documentos son a menudo la propiedad más preciada que un hombre puede tener» (Cedric Laurant, 2012: 20).

6. En el año 1763, el parlamentario William Pitt señaló en su discurso sobre el proyecto de Ley de Impuestos Especiales que «el hombre más pobre en su rústica vivienda puede ofrecer resistencia a todo el poder de la Corona. Su vivienda podría ser precaria; su techo podría temblar; el viento podría soplar a través de éste; las tormentas podrían ingresar; la lluvia podría pasar, pero el Rey de Inglaterra no puede entrar; todas sus fuerzas no se atreven a cruzar el umbral de la casa en ruinas» (Cedric Laurant, 2012: 20).

mulgó la Ley de Acceso a los Registros Públicos, la cual estableció que la información en manos del gobierno debía ser utilizada para propósitos legítimos (Cedric Laurant, 2012: 20), mientras que en Francia, en el año 1858, se prohibió la publicación de hechos privados fijando fuertes multas para quienes infringieran estas prohibiciones, y Noruega estableció en 1889 una norma que prohibía la publicación de información relativa a «asuntos personales o domésticos» (Cedric Laurant, 2012: 20).

Pese a lo anterior, debemos convenir que no fue sino hasta la publicación de «The Rigth to Privacy» que por primera vez se dio una definición del derecho a la privacidad, entendiéndola como el derecho a no ser molestado o «the right to be let alone» (Warren y Brandeis, 1995: 44).

CONCEPTO DEL DERECHO A LA PRIVACIDAD

Es importante señalar que el derecho a la privacidad del que hablaban Warren y Brandeis no es un concepto unívoco, al contrario, ha resultado de difícil precisión. Así, por ejemplo, en el caso de los países hispanohablantes, cuando se habla del «right to privacy» se tiende a hablar indistintamente del derecho a la «privacidad», a la «intimidad» y a la «vida privada». Por lo demás, su noción no es la misma en uno u otro país, debido a los diversos niveles socioculturales. En Estados Unidos el derecho a la privacidad se origina en el rechazo de la intromisión no autorizada de los medios de comunicación y del Estado en la vida privada. Si bien en este país no se reconoce expresamente en la Constitución el derecho a la privacidad, su desarrollo jurisprudencial ha permitido resguardar diversos bienes jurídicos que se relacionan con el «right to privacy», razón por la que este derecho sólo se concede a expensas de otras libertades, entre ellas las libertades de expresión, de asociación, sexuales, entre otras,[7] resultando por ello un concepto más amplio que en otros países.

7. Cabe señalar que si bien no se reconoce expresamente el derecho a la privacidad en la Constitución de Estados Unidos, la autora María Nieves Saldaña señala que «el derecho a la privacidad es único en el sistema constitucional de los Estados Unidos, puesto que sólo puede concederse a expensas de otras libertades fundamentales reconocidas expresamente en la Constitución norteamericana, unidas y entrelazadas de forma inextricable por el mismo derecho a la privacidad. Así, la Primera, Cuarta, Quinta, Novena y Decimocuarta Enmiendas dan fundamento a distintas facetas de privacidad, de forma que constitucionalmente el derecho a la privacidad está vinculado a cuatro de las diez

Sumado a las dificultades anteriores, debe añadirse que el alcance y contenido de este derecho cambia con el transcurso del tiempo. Así, por ejemplo, en los años sesenta y setenta, con el arribo de nuevas tecnologías que permitieron recolectar, procesar y analizar información, las personas se vieron expuestas a diversos riesgos de injerencia por parte de terceros y de las autoridades, y por ello se reconoció, en ese contexto, que el derecho a la privacidad tenía no sólo una dimensión negativa, entendida como el poder de excluir del conocimiento ajeno aquello que se refiere a la propia persona (Herrán, 2002: 24), sino que también una dimensión positiva referida al poder de controlar y vigilar la información que otros poseyeran respecto de terceros (Herrán, 2002: 24; Cedric Laurant, 2012: 22). Esto generó normas específicas para el resguardo de la información de las personas, regulando con ello la recolección, almacenamiento, acceso y manejo de la información, lo que dio origen al derecho a la protección de datos personales.

Ahora bien, como es evidente desde los años sesenta hasta la actualidad, las tecnologías han evolucionado exponencialmente. Hoy existen miles de archivos electrónicos, bases de datos públicas y privadas en las cuales se dispone de datos personales generales e incluso datos sensibles,[8] y es posible hallar grandes cantidades de información relativa a terceras personas, pudiendo incluso encontrarse almacenada en objetos tan cotidianos como nuestras cédulas de identidad. Pese a ello, y aun cuando la información contenida en la mayoría de estos repositorios de información ha sido proporcionada principalmente por nosotros mismos, esto no significa que no exista privacidad. En este sentido el profesor Renato Jijena Leiva ha señalado que:

> No es que la intimidad no exista, sino que ella ha cambiado. Cuando fue concebida en 1870, se le definió —desde una concepción indivi-

primeras Enmiendas, a cinco de las catorce primeras, y las 'emanaciones derivadas de las zonas de penumbra' a todo el Bill of Rights» (Saldaña, 2011: 309).

8. La Ley 19.628 sobre Protección de la Vida Privada, también conocida como Ley de Protección de Datos Personales, define datos sensibles como «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».

> dualista— como el «right to be let alone» o derecho de ser dejado a solas [...] Hoy en día, atendida la fuerte penetración de los sistemas electrónicos de procesamiento de información o informáticos, se le debe concebir desde una óptica socializadora. Se han formulado el llamado «Principio de la autodeterminación informativa» y el «habeas data o derecho de acceso», para sostener que de cara al siglo XXI las personas, si bien es cierto no pueden oponerse absolutamente al procesamiento de datos personales, tienen derecho a poder controlar y autodeterminar el uso que se haga del conjunto de datos o antecedentes personales que se relacionan con su esfera íntima [...], tanto por órganos públicos o la Administración del Estado como por empresas particulares (Jijena Leiva, 2015).

De esta forma, por medio del procesamiento de datos, los cuales pueden ser tratados (es decir, recopilados, almacenados, cruzados, etcétera) indebidamente, es posible tener un enorme conocimiento de la esfera privada de una persona. Es así como hoy las tecnologías han hecho posible mediante la recolección y análisis de datos la creación de cuadros completos de la vida de una persona, sobre todo de aspectos que nunca tuvo la intención de revelar (Greenwald, 2014: 260).

Es importante señalar que, si bien existe una tendencia a regular normativamente la protección de datos personales y la privacidad de forma independiente,[9] nosotros somos de la opinión de que la protección de datos personales está en una relación de género a especie con la privacidad, siendo la «privacidad» el género y la «protección de datos

9. Respecto a esto, el *Informe de privacidad y derechos humanos* nos señala que «la génesis de la legislación moderna en esta área puede ser rastreada hasta la primera ley de protección de datos en el mundo promulgada en el Estado Federado de Hesse en Alemania en 1970. Ello fue seguido por leyes nacionales en Suecia (1973), los Estados Unidos de América (1974), Alemania (1977) y Francia (1978). Dos instrumentos internacionales fundamentales se desarrollaron a partir de estas leyes. La Convención para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa en 1981 y las Directrices que Gobiernan la Protección de la Privacidad y el Intercambio Transfronterizo de Datos Personales de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) fijan normas específicas que se ocupan del manejo de datos electrónicos. Estas normas describen a la información personal como datos a los que se les suministra protección desde su recolección hasta su almacenamiento y difusión» (Cedric Laurant, 2012: 22).

personales» la especie. En este sentido, si consideramos que los datos personales pueden servir para la confección del perfil de una persona, permitiendo así conocer su ideología, raza, orientación sexual, identidad de género, situación económica, salud o cualquier otra información de su persona, lo que realmente ocurre es que ese perfil constituye una construcción de la esfera privada del sujeto. De allí que la capacidad de controlar nuestra información deba ser entendida como parte del concepto de privacidad.

Por su parte, cabe señalar que el derecho a la privacidad ha sido reconocido como un derecho humano tal como dan cuenta numerosos instrumentos internacionales.[10] En este sentido, resulta irrelevante si denominamos este derecho con las voces «privacidad», «intimidad» o «vida privada» siempre que comprendamos el contenido y alcance de este derecho.

Un concepto de derecho a la privacidad debe ser entendido de la forma más amplía, de modo que resguarde la dignidad y libertad de la personas, evitando que terceros la afecten mediante su intromisión arbitraria e ilegal de cualquier tipo. Con esto no se reconoce un derecho absoluto, sino que, por el contrario, cada vez que se deba establecer limitaciones a él, los Estados deberán resguardar que las intromisiones que se permitan sean fijadas en la ley conforme a estándares mínimos que no resulten atentatorios contra los derechos de las personas.

CONCEPTO DE DERECHO A LA PRIVACIDAD EN CHILE

En nuestro país, la Constitución Política utiliza la voz «vida privada» en el artículo 19 número 4, voz que ha sido caracterizada por su difícil precisión en la doctrina, como lo ha señalado, entre otros, el profesor Rodolfo Figueroa, quien ha sintetizado varias de esas definiciones en el siguiente extracto:

> Es entendido [...] intimidad en el sentido de conciencia, como el derecho a estar solo, esto es, apartado de observación (lo que podemos

10. Algunos de ellos son la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Convenio Europeo para la Protección de los Derechos Humanos y Libertades fundamentales, la Convención Americana sobre Derechos Humanos, entre otros.

> llamar *seclusión* o tranquilidad); como secreto; como un ámbito de no injerencia; como autodeterminación y autonomía; como el derecho a restringir información sobre uno mismo; como territorialidad, lo que comprende seclusión y secreto, y también como un derecho a la imagen. Es evidente que algunas de estas nociones se superponen o implican entre sí (Figueroa, 2013: 860).

Cabe señalar que en Chile se reconoce el derecho a la privacidad como un derecho dinámico y por tanto sus ámbitos de protección varían conforme a la evolución de nuestra sociedad. Así, el profesor Tomás Vial ha señalado que «el derecho de privacidad es un derecho especialmente evolutivo, pues sigue muy de cerca las costumbres, hábitos y moral de cada sociedad en particular» (2000: 51), agregando que debido a esto «cuando se lo estudia con respecto a nuevas circunstancias de la vida colectiva, lo verdaderamente relevante es saber si aquellas circunstancias corresponden al sentido garantístico que la norma tiene» (2000: 51).

Debido a lo anterior el trabajo que hacen algunos autores[11] a la hora de distinguir categorías o ámbitos comprendidos por el derecho a la privacidad es vital para entender que este derecho tiene un alcance y contenido que es principalmente evolutivo, ya que esas categorías pueden ir ampliándose junto con la noción de este derecho.

EL DERECHO A LA PRIVACIDAD EN EL ORDENAMIENTO JURÍDICO DE CHILE

El profesor Humberto Nogueira Alcalá ha señalado que en Chile contamos con un bloque constitucional, el que está compuesto por distintas normas que confluyen en materias de derechos humanos (Nogueira Alcalá, 2007: 459-461), idea que recientemente fue reconocida por el propio Tribunal Constitucional de Chile,[12] lo que supone resguardar también el derecho a la privacidad.

Así, como punto de partida, debemos mencionar que la Constitución establece en su capítulo uno las bases de la institucionalidad, indicando

11. En relación a los intentos de categorización del derecho de privacidad encontramos a los siguientes autores en Chile: Anguita (2006: 319-521), Figueroa (2013: 863-883), Rodríguez Pinto (1999: 719-744), Gómez (2005: 322-419) y Tapia (2008: 117-144).

12. Sentencia del Tribunal Constitucional de 6 de mayo de 2014, rol 2493-13, considerandos sexto y séptimo.

los valores o principios básicos que deben guiar no sólo el actuar del Estado, sino que también a las personas y entidades privadas.[13]

Ahora, respecto a las disposiciones que se vinculan directamente al derecho a la privacidad y que conformarían parte del bloque constitucional de este derecho, encontramos los numerales 4 y 5 del artículo 19. Si bien la redacción de estos numerales y el contenido de los mismos pareciera indicar que protegen bienes jurídicos distintos, la verdad es que ambos corresponden a la protección del derecho a la privacidad.[14]

Cabe señalar que, además de las disposiciones previamente mencionadas, forman parte de este bloque constitucional, en conformidad al artículo 5 de la Constitución, todas aquellas normas de *ius cogens*, derecho internacional consuetudinario y tratados internacionales reconocidos y ratificados por Chile.

CONTENIDO Y ALCANCE DEL DERECHO A LA PRIVACIDAD EN INTERNET EN CHILE

Configurado nuestro bloque constitucional del derecho a la privacidad, cabe analizar el contenido y alcance de este derecho. Esto nos permitirá establecer, en forma general, qué es aquello que debe protegerse para

13. Al respecto, el Tribunal Constitucional ha señalado que «el contenido del artículo 19 [de la Constitución], conjuntamente con sus artículos 1, 4 y 5, inciso segundo, configuran principios y valores básicos de fuerza obligatoria que impregnan toda la Constitución de una finalidad humanista que se irradia en la primacía que asignan sus disposiciones a la persona humana, a su dignidad y libertad natural, en el respeto, promoción y protección a los derechos esenciales que emanan de la naturaleza humana, que se imponen como deber de los órganos del Estado». Añade a su vez que «estos principios y valores no configuran meras declaraciones programáticas sino que constituyen mandatos expresos para gobernantes y gobernados, debiendo tenerse presente que el inciso segundo del artículo 6 de la Constitución precisa que los preceptos de ésta obligan no sólo a los titulares o integrantes de los órganos del Estado, sino a toda persona, institución o grupo» (Sentencia del Tribunal Constitucional de 16 de abril de 2009, rol 1185-08, considerandos undécimo y duodécimo).

14. Así lo ha señalado también el profesor Hernán Corral, quien el año 2001, antes de la última reforma Constitucional del año 2005, señalaba que el número 5 del artículo 19 que se refería a la inviolabilidad del hogar, de las comunicaciones y documentos privados no era más que una especificación del derecho al respeto y protección de la vida privada: «bien podría haberse prescindido de esta especificación ya que la sola consagración del derecho a la vida privada la incluía» (Corral, 2001: 206).

que efectivamente se pueda resguardar la dignidad y la libertad de las personas en internet.

Que internet sea un lugar sin mayores restricciones de acceso y por lo general abierto a todos, no significa que las personas no puedan tener espacios donde puedan apartarse de la observación ajena. En este sentido, el Tribunal Constitucional señaló recientemente que «la intimidad no sólo puede darse en los lugares más recónditos, sino que también se extiende, en algunas circunstancias, a determinados espacios públicos donde se ejecutan específicos actos con la inequívoca voluntad de sustraerlos a la observación ajena».[15] Luego, el Tribunal Constitucional en relación a internet agrega 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».[16]

En ambos extractos la idea a la que se refiere el Tribunal Constitucional se puede denominar como la expectativa de privacidad de las personas, entendiéndose por esto a la legítima y razonable expectativa que transciende a catalogar un espacio o lugar como público o privado, pues lo que importa es la subjetividad del individuo (Álvarez, 2013).

Ahora, es importante mencionar que a nuestro entender 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. Así, por ejemplo, cuando entregamos información personal en redes sociales, esa información sigue siendo privada mientras tengamos la expectativa de que esa información no será utilizada por terceros.

Siguiendo este mismo orden de ideas, es dable citar el caso sucedido en el año 2012 en el que se presentó una acción de protección por un funcionario de Carabineros, quien recurrió en contra de la resolución que lo eliminó de las filas de la institución por haber posteado un co-

15. Sentencia del Tribunal Constitucional del 12 de julio de 2014, rol 1894-11, considerando vigésimo tercero.

16. Sentencia del Tribunal Constitucional del 12 de julio de 2014, rol 1894-11, considerando vigésimo tercero.

mentario en contra de su superior en su cuenta privada de Facebook. En el recurso, el funcionario alude a que se habrían vulnerado algunos de sus derechos fundamentales, entre ellos el consagrado en el número 4 del artículo 19 de la Constitución, ya que se habría obtenido información publicada en su cuenta privada de Facebook, agregando además que dicha información habría sido obtenida sin autorización judicial.

La Corte de Apelaciones de Temuco rechazó el recurso señalando para ello que lo expuesto en Facebook se habría obtenido por comentarios de terceros hacia los superiores del recurrente y no por el hecho de que la institución o el recurrido hubiera obtenido alguna clave para ingresar al Facebook del actor, lo que según la Corte hubiese violado su privacidad. Luego la Corte remarcó el hecho de que el recurrente efectivamente habría posteado el comentario, siendo esto último determinante ya que esto expuso a un número determinado de personas sus comentarios, sin que hubiese existido prohibición alguna para que los que lo vieran pudieran comentarlo con otras personas, razón por la cual decidió rechazar el recurso.[17]

La Corte Suprema, por su parte, confirmó la sentencia apelada. Pese a ello es importante destacar el voto disidente del ministro Sergio Muñoz, quien estuvo por rechazar la sentencia apelada y acoger el recurso de protección. Para ello el ministro se refirió a las características de Facebook, señalando así que éste «es un sitio web que permite a sus usuarios comunicarse e intercambiar opiniones entre ellos, para lo cual el interesado debe solicitar autorización expresa a un tercero para incorporarlo en sus contactos y dicho tercero sólo se integrará a los mismos luego de consentir expresamente en ello».[18] Debido a lo anterior, sostiene que sólo entre quienes ha existido esta autorización la información y sus comunicaciones son públicas, no existiendo por ello una habilitación para que dicha información sea utilizada por otras personas que no han sido autorizadas.

Finalmente, el ministro Muñoz sostiene que si bien la garantía constitucional aludida por el recurrente puede ser afectada previa habilitación legal por la autoridad competente y siguiendo el procedimiento pertinen-

17. Sentencia de la Corte de Apelaciones de Temuco del 28 de junio de 2012, rol 684-2012.

18. Voto disidente del ministro Muñoz, Corte Suprema, rol 5.322-2012.

te, esto en el caso en cuestión no ocurrió ya que el acceso a las publicaciones realizadas por el recurrente habría sido ilegítimo y, en consecuencia, según sus palabras «la autoridad de Carabineros no podía acceder a ella ni menos utilizarla como fundamento de una sanción disciplinaria, más aún cuando no se señala en el informe, emitido en su oportunidad, de quién se obtuvo dicha información, constituyéndose en consecuencia en prueba ilícita y por ende no susceptible de ser utilizada».[19]

Lo anterior da cuenta de que el derecho a la privacidad no es absoluto y puede ser limitado, pero para ello se deben cumplir ciertos requisitos, los cuales deben mantener fuertes controles de razonabilidad y proporcionalidad en su aplicación. De lo contrario los ámbitos de protección de este derecho se desvanecen junto con el resguardo a las expectativas de la privacidad en internet.

En la actualidad, debido a las libertades que nos facilita internet, el ejercicio democrático se ha visto fuertemente beneficiado: existe más información, transparencia, y la posibilidad de un mayor número de discursos. Sin embargo, con el objeto de perseguir fines legítimos —como combatir la pornografía infantil, el terrorismo o el narcotráfico— los países se han visto en la necesidad de restringir la privacidad en la web, tomando medidas como la vigilancia en internet.

Pese a lo legítimo que puedan ser los objetivos, estas restricciones no deben ser permitidas *per se,* debido al peligro que puede significar para nuestra privacidad. En este sentido, el Tribunal Constitucional, en su sentencia respecto al proyecto de ley en contra de la pornografía infantil, el cual contemplaba un sistema de registro de los usuarios de cibercafé, señaló:

> Dicha intimidad resultaría usurpada en caso de seguimientos o monitoreos sistemáticos, constantes y focalizados para husmear a qué lugares asiste alguien, por pertenecer a una categoría a priori sospechable de ciudadanos; por dónde —vías, caminos o canales— se desplaza en particular; cuál es el número de los sitios que visita y de las direcciones contactadas, precisamente; con quién, o con cuánta duración y frecuencia se producen las conexiones realizadas. Más todavía cuando, a partir de estos datos, hoy es factible ir de hurones e inferir historiales o perfiles individuales, que incluyen hábitos y patrones de conducta humana,

19. Voto disidente del ministro Muñoz, Corte Suprema, rol 5.322-2012.

> hasta poder revelar las preferencias políticas, opciones comerciales e inclinaciones sociales de las personas (considerando vigésimo segundo, sentencia número 1894-11).

Los monitoreos sistemáticos a los que se refiere el Tribunal Constitucional, los cuales se reprochaban en ese entonces entendidos como vigilancia en internet, han generado bastante discusión en el último tiempo y es aquello lo que justifica este artículo. Si bien, tal como se desprende de las citas señaladas, nuestra jurisprudencia reconoce que el derecho a la privacidad, resguarda un espacio en el cual las personas tienen una expectativa de privacidad, y que si bien este derecho no es absoluto, para ser restringido debe cumplirse con ciertos requisitos, que se explicitarán más adelante.

VIGILANCIA EN INTERNET: ¿INTROMISIÓN LEGÍTIMA O ILEGÍTIMA EN EL SISTEMA NORMATIVO CHILENO?

¿QUÉ ES LA VIGILANCIA?

Respecto de la voz *vigilancia*, las teorías sociales han señalado que existen diversos tipos de conceptos, entre ellos los neutrales y negativos. Cuando hablamos de los conceptos neutrales, Fuchs señala que los supuestos del concepto neutral de vigilancia serían que: i) la vigilancia posee aspectos positivos; ii) que tiene dos caras, por un lado permisiva y por otro restrictiva; iii) la vigilancia es un aspecto fundamental para todas las sociedades; iv) la vigilancia es necesaria para la organización; y v) que cualquier tipo de compilación sistemática de información es vigilancia (Fuchs, 2011: 135).

Ahora bien, si aplicamos estos supuestos a las actividades comunes que ocurren en internet, el resultado sería que todas las formas de almacenamiento, procesamiento y uso de la información revestirían las características de vigilancia. De este modo, el concepto neutral de vigilancia parece ser bastante amplio, por lo que de acuerdo a Fuchs esto impediría establecer una correcta concepción de «vigilancia en internet» (Fuchs, 2011: 135).

En el caso de los conceptos negativos,[20] Fuchs señala que la vigilancia

20. Fuchs indica a su vez que los conceptos negativos de vigilancia más conocidos son aquellos dados por Michel Foucault, quien la vería como una forma de poder disciplinario (Fuchs, 2011: 136)

consistiría en una forma de recopilación sistemática de información y que ésta se relacionaría a la dominación, coerción o a la amenaza de utilizar la violencia con el objeto de alcanzar ciertas metas y acumular poder, lo cual se haría en muchas ocasiones en contra de la voluntad y conocimiento de quienes están siendo vigilados (Fuchs, 2011: 136). Mencionado esto, Fuchs nos señala que él prefiere definir la vigilancia como un concepto negativo, principalmente por las siguientes razones:

a) *Etimológica*. Para él la palabra *surveillance* viene de la palabra en francés *surveiller,* la cual significa «supervisar» o «vigilar». De esta forma, él entiende que esta palabra implica una jerarquía y, por lo tanto, estaría conectada a nociones como observador, vigilantes, supervisor y oficial. Por lo que vigilancia debe ser concebida según las palabras de Foucault como una técnica de coerción, como un poder ejercido sobre una persona mediante una supervisión (Fuchs, 2011: 136).

b) *Conflacionismo teórico*.[21] Para Fuchs los conceptos neutrales de vigilancia podrían ser usados para la legitimación de formas coercitivas de vigilancia, sosteniendo que la vigilancia es omnipresente y, por ende, exenta de problemas, razón por la cual ciertas situaciones, como cuidar de un bebé o como el electrocardiograma de un paciente de infarto de miocardio, se encontrarían en el mismo nivel que fenómenos muy diversos, como la vigilancia preventiva del Estado de los datos de los ciudadanos para combatir el terrorismo o la vigilancia económica de datos privados o del comportamiento por compañías de internet para acumular capital con la ayuda de publicidad direccionada (Fuchs, 2011: 136).

c) *Diferencia entre recopilación de información y vigilancia*. Respecto a este punto, Fuchs señala que si la vigilancia fuera concebida como recopilación sistemática de información, ésta no podría entenderse diferenciada entre los estudios de vigilancia y los estudios de la sociedad de la información y entre una sociedad vigilada y una sociedad de la información. El autor entiende que en estas circunstancias no habría ningún motivo para reclamar la existencia de estudios de vigilancia como disciplina o transdisciplina (Fuchs, 2011: 136).

d) *La normalización de la vigilancia*. Finalmente, el autor postula que

21. El autor se refiere a «*theoretical conflationism*», la palabra «*conflation*» traducida al español significa conflación, que según el Diccionario de la Real Academia de la Lengua Española significa acción o efecto de fundir.

si consideramos que todo es vigilancia, entonces se vuelve muy difícil criticar la vigilancia coercitiva política (Fuchs, 2011: 136).

Debido a estos argumentos, Fuchs llega a la conclusión de que conviene dar un concepto de vigilancia negativo, entendiéndola como «la recolección de información de individuos o grupos que es usada para controlar o disciplinar el comportamiento mediante la amenaza de ser objetos de violencia» (Fuchs, 2011: 136).

Desde nuestro punto de vista, entender la vigilancia desde una concepción negativa como lo hace Fuchs tendría como consecuencia no considerar como vigilancia formas de observación sistemática a las que podrían estar sujetas las personas, pero que hasta que no se califique su uso no lo serían, lo cual nos parece errado. En cambio, la concepción neutral, si bien es más amplía, nos permite comprender que en realidad hoy en día somos sujetos de una vigilancia constante, pese a que posteriormente sea o no utilizada contra nosotros la información que se recopila y almacena.

Dicho lo anterior, es necesario referirnos a la vigilancia en internet. En primer lugar debemos especificar que este trabajo se centra en la vigilancia que ha dado lugar al surgimiento de la denominada web 2.0.[22] En el momento en que se acuñó este concepto, se señalaron ciertas características que ayudarían a diferenciar aquellas plataformas de la web 1.0, siendo una de sus principales características la posibilidad de generar tanto comunicación, interacción y participación de forma colaborativa. Ahora, además hay que considerar que la web 2.0 tiene otra característica importante: la capacidad de almacenar, procesar, valorar y vender grandes cantidades de información personal y del comportamiento de los usuarios (Fuchs, 2011: 137).

Desde el surgimiento de la web 2.0, se han generado nuevas discu-

22. Tim O'Reilly señala que para considerar una aplicación o plataforma como una web 2.0 sería necesario que cumpliera con algunas características, señalando así las siguientes: servicios en lugar de software empaquetado, con escalabilidad rentable; control sobre fuentes de datos exclusivas y difíciles de recrear, que se enriquecen cuanto más gente las utiliza; confianza en los usuarios como codesarrolladores; aprovechamiento de la inteligencia colectiva; aprovechamiento de la larga cola mediante el autoservicio de los clientes; el software por encima del nivel de un único dispositivo; ligereza en la interface de usuario, en los modelos de desarrollo y en los modelos de negocio (O'Reilly, 2007: 36-37).

siones acerca de la vigilancia y la privacidad de los usuarios de estas plataformas. Adicionalmente, las declaraciones de Edward Snowden han permitido despejar dudas acerca de la existencia de programas de vigilancia, tales como el sistema PRISM,[23] el cual permitiría tener acceso a la información personal de millones de usuarios de empresas de publicidad, comunicaciones y de medios sociales alrededor del mundo.

Años atrás, sin embargo, ya se hablaba de las repercusiones que podría tener la web 2.0. Una de las personas que alertaba de ello era Roger Clarke (1994), quien en ese entonces hacía la distinción entre vigilancia de datos personales y entre vigilancia masiva de datos. Así, señalaba que la primera consistía en la vigilancia respecto de las acciones de una o más personas, mientras que la segunda consistía en la vigilancia respecto de un grupo o una población.

Manuel Castells (2009), por su parte, se refirió a las características principales de las web 2.0, a las cuales identificó como «mass self-communications», para referirse a la posibilidad de alcanzar eventualmente a una audiencia global y a la información que éstas recopilan y comunican, que es la información que sus mismos usuarios crean.

Fuchs, tomando en consideración lo señalado por Castells y Clarke, se refiere a la vigilancia web 2.0 como aquella que «está dirigida a grandes grupos de usuarios, quienes ayudan a producir y reproducir hegemónicamente vigilancia al proveer contenido generado por los usuarios (autoproducido)» (Fuchs, 2011: 138).

Es así como, en la actualidad, la información de los usuarios de internet traza el siguiente recorrido: en primer lugar se externaliza y se hace pública o semipública en la web, lo que posibilita la comunicación *online* de los usuarios; luego, se privatiza dicha información por los proveedores de servicios de internet, para obtener beneficios de ella; y, finalmente, esta información puede también llegar a manos de servicios secretos o autoridades de los Estados, quienes gracias a la web 2.0 pueden llegar a tener inmensas cantidades de información bajo su control. Ahora, cabe precisar que cuando hablamos de esta información no nos referimos so-

23. De acuerdo a lo señalado por Edward Snowden, el programa PRISM de la Agencia de Seguridad Nacional de Estados Unidos permite tener acceso directo a la información de los usuarios desde nueve empresas de comunicación: AOL, Apple, Facebook, Google, Microsoft, Paltalk, Skype, Yahoo y Youtube (Greenwald, 2014: 133).

lamente al contenido o mensaje, sino que también a los datos asociados a aquéllos o, más bien, a los denominados metadatos.[24]

La privacidad no se encuentra limitada al contenido de nuestras comunicaciones. Los metadatos pueden entregar información incluso más completa que una conversación telefónica aislada. Greenwald explica los beneficios de los metadatos versus el contenido de una comunicación en los siguientes términos:

> Imaginemos el caso de una mujer que llama a una clínica donde se practican abortos. La escucha secreta de su llamada telefónica quizá revele sólo la concertación o confirmación de una cita en una clínica con un nombre genérico («Clínica del East Side» o «consultorio del doctor Jones»). Sin embargo, los metadatos dejan ver mucho más: la identidad de las personas que reciben la llamada. Lo mismo sucede con las llamadas a un especialista en VIH, a un centro de gays y lesbianas o a una línea de ayuda a suicidas. Los metadatos también descubrirán una conversación entre un activista de los derechos humanos y un informante de un régimen represivo o a una fuente confidencial que revelará a un periodista fechorías de alto nivel. Si uno llama con frecuencia a última hora de la noche a alguien que no es su cónyuge, los metadatos lo reflejarán. Es más, en ellos quedará constancia no solo de las personas con quien uno intenta comunicarse y la frecuencia, sino también de todas las personas con las que se comunican sus amigos y colegas, lo que genera un cuadro exhaustivo de la red de relaciones (Greenwald, 2014: 166).

Greenwald se refiere luego a las palabras del profesor de ciencia informática de la Universidad de Princeton Edward Felten, quien durante una declaración jurada ante la American Civil Liberties Union explica la razón del beneficio de los metadatos sobre el contenido de las comunicaciones, señalando por ejemplo que las escuchas secretas de llamadas podían resultar bastante difíciles producto de las diferencias lingüísticas, del uso de argot o de códigos, a las divagaciones y a otras cuestiones que, de forma deliberada o por casualidad, podrían confundir el significado

24. La definición de metadato, según José Senso y Antonio de la Rosa, «es toda aquella información descriptiva sobre el contexto, calidad, condición o características de un recurso, dato u objeto que tiene la finalidad de facilitar su recuperación, autentificación, evaluación, preservación o interoperatividad» (2003: 99).

de las palabras. En cambio, el profesor señala que los metadatos son matemáticos, por ello nítidos, precisos y, gracias a esto, fáciles de analizar. De este modo, de acuerdo a las palabras de Felten, la recolección masiva de datos permitiría también enterarse de hechos nuevos y privados de los que nunca se podrían haber enterado de otra forma (Greenwald, 2014: 165-167).

De esta forma, el surgimiento de la web 2.0 ha tenido como resultado que mediante la recolección, combinación y evaluación de la información que los usuarios comunican, los controladores de dicha información puedan obtener una visión detallada de la vida, secretos y preferencias de los usuarios.

Cabe señalar que debido a la evolución constante que han tenido las tecnologías en los últimos años, el hecho de que hoy exista una web 2.0 no impide que surja una web que posea nuevas características, razón por la que la vigilancia a la que nos referimos es aquella que se realiza por medio de internet utilizando para ello las tecnologías de la información y no se restringe solamente a la que ocurre utilizando las plataformas de la web 2.0.

Dicho lo anterior, la vigilancia en internet a la que nos referimos en este trabajo debe ser entendida 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 tipos de información que son recopilados, almacenados y eventualmente analizados para determinar actos, conductas, preferencias, localización y otras características que permitirán individualizar a los usuarios.

Ahora bien, tal como adelantamos en la introducción, este artículo se centra en la vigilancia en internet ejercida o utilizada por el Estado y sus instituciones con la finalidad de resguardar el orden, la prevención del delito y la seguridad del Estado y sus habitantes en general. De modo que no contempla el análisis de la vigilancia privada en el contexto de los servicios de seguridad privada por exceder el objeto de la investigación.

Considerando lo anterior, a continuación nos referiremos al marco normativo de nuestro ordenamiento jurídico que se relaciona con las medidas de intromisión que pueden ser consideradas como vigilancia en internet del Estado.

MARCO LEGAL DE LA INTROMISIÓN A LA PRIVACIDAD EN EL ORDENAMIENTO JURÍDICO CHILENO

En nuestro ordenamiento encontramos varias normas que permiten llevar a efecto diligencias que restringen la privacidad, todas ellas tienen las siguientes características en común: i) que se encuentran establecidas por ley; ii) que se establecen obligaciones de guardar reserva de la información obtenida; iii) que requieren ser solicitadas y concedidas por razones fundadas; y iv) que se establece una finalidad al uso de la información obtenida. Dentro de estas normas podemos señalar, a modo de ejemplo, las siguientes.

Ley Orgánica Constitucional del Ministerio Público (LOCMP)

Establece el principio de objetividad, señalando expresamente que el Ministerio Público podrá impartir órdenes directas a las Fuerzas de Orden y Seguridad durante la investigación. Sin embargo, señala que cuando las actuaciones priven, restrinjan o perturben al imputado o a un tercero en el ejercicio de sus derechos fundamentales se requerirá aprobación judicial previa.

Código Procesal Penal (CPP)

Al igual que la LOCMP, contempla expresamente el principio de objetividad. Específicamente respecto a intromisiones a la privacidad, el CPP establece procedimientos y requisitos legales específicos que las autoridades deberán realizar a la hora de efectuar cada uno de ellos. Ahora, sólo nos referiremos a algunas intromisiones que resultan especialmente relevantes para nuestro estudio; pese a ello, debemos destacar que en ningún caso el legislador se ha preocupado de definir cada uno de estos actos, lo que genera redundancias:

- La retención e incautación de correspondencia (artículo 218 del CPP). En conformidad a ello, el fiscal podrá solicitar fundadamente al juez la retención e incautación de la correspondencia del imputado o dirigida a él, incluso podría hacerlo antes de que la investigación esté formalizada. Respecto a esta norma, la ley es bastante amplia al referirse a la correspondencia; pareciera sólo

referirse a la correspondencia física, sin embargo, esto queda subsanado al permitir la obtención de copias o respaldos de la correspondencia electrónica. El CPP a su vez contempla una restricción respecto a la conservación de los documentos obtenidos, siendo posible hacerlo sólo cuando tuvieren relación con el hecho objeto de la investigación.

- La obtención de copias de comunicaciones o transmisiones (artículo 219). En conformidad con este artículo, el fiscal podrá solicitar a cualquier empresa de comunicaciones la obtención de copias de comunicaciones o transmisiones, pudiendo también ordenar la entrega de las versiones que existieren de las transmisiones de radio, televisión u otros medios. A primera vista, y al igual que la medida anterior, ésta parece ser bastante amplia, ya que incluso coincide con la norma anterior al permitir la obtención de la correspondencia electrónica, toda vez que la correspondencia electrónica y la digital no parecieran diferir.
- La intercepción de comunicaciones telefónicas o de otras formas de telecomunicación[25] (artículos 222 y 369 ter[26]). Esta norma permite al fiscal solicitar que se autorice la interceptación y grabación de las comunicaciones telefónicas o de otras formas de telecomunicación, tanto del imputado como de terceros que puedan haber estado relacionados con los hechos ilícitos que fundamentan la solicitud. A su vez, establece una obligación para las empresas telefónicas y de comunicaciones, las que deberán llevar un listado

25. Si bien el CPP no define la voz *telecomunicación*, la Ley General de Telecomunicaciones sí lo hace en su artículo 1, entendiendo por telecomunicación toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos e informaciones de cualquier naturaleza, por línea física, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.

26. Este artículo fue añadido con la Ley 19.927 que modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal en materia de delitos de pornografía infantil, en el cual establece expresamente que en caso de los delitos de esa especie se podrá autorizar la interceptación o grabación de las telecomunicaciones de esa persona o de quienes integraren dicha organización, la fotografía, filmación u otros medios de reproducción de imágenes conducentes al esclarecimiento de los hechos y la grabación de comunicaciones. Mismas formas de intromisión ya contempladas por el CPP.

actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a seis meses, de los números IP de las conexiones que realicen sus abonados, registro que tendrá carácter reservado y que estará a disposición del Ministerio Público.

- Registro de la interceptación telefónica y de otras formas de comunicación (artículo 213 del CPP). El CPP faculta el registro de estas interceptaciones y señala expresamente que se podrán hacer mediante su grabación magnetofónica u otros medios técnicos análogos que aseguren la fidelidad del registro. Cabe señalar que se permite incluso que estas interceptaciones puedan ser transcritas por un funcionario que actuará, en tal caso, como ministro de fe acerca de la fidelidad del texto.
- Medidas de vigilancia (artículo 213 del CPP). El CPP utiliza expresamente la voz *vigilancia*, sin embargo, no la precisa mediante definición alguna, sino por el contrario permite expresamente al fiscal ejercer todas las medidas de vigilancia que estime conveniente para evitar la fuga del imputado o la sustracción de documentos o cosas que constituyeren el objeto de la diligencia. Ahora, si bien esta norma no señala expresamente que deba solicitar autorización al juez para llevar a efecto algunas de estas medidas, el fiscal está obligado a hacerlo cuando se pueda restringir, perturbar o privar un derecho constitucional como el derecho a la privacidad.

Ley 18.314 que Determina Conductas Terroristas y Fija su Penalidad (Ley de Terrorismo)

En ella se establece una lista de delitos cuya finalidad sería la de producir en la población, o en una parte de ella, el temor justificado de ser víctima de delitos de terrorismo. A su vez, faculta al juez de garantía respectivo autorizar al Ministerio Público para que éste pueda llevar a cabo distintas medidas, entre las que encontramos las de interceptar, abrir o registrar las comunicaciones telefónicas e informáticas y la correspondencia epistolar y telegráfica, siendo necesaria la autorización judicial. Ahora, esta ley tampoco define cada uno de estos actos.

Ley 19.974 sobre el Sistema de Inteligencia del Estado y crea la Agencia Nacional de Inteligencia (Ley de Inteligencia)

Esta ley se aplica a toda la actividad de inteligencia y contrainteligencia que realicen los órganos y servicios que integren su sistema. A su vez, define sus objetivos generales señalando que es proteger la soberanía nacional y preservar el orden constitucional. Luego, distingue entre los servicios de inteligencia militar y los servicios de inteligencia policial. Respecto a los primeros, señala que comprenderían principalmente la inteligencia y contrainteligencia necesaria para detectar, neutralizar y contrarrestar, dentro y fuera del país, las actividades que puedan afectar la defensa nacional y que corresponden a las Fuerzas Armadas y a la Dirección de Inteligencia de Defensa del Estado Mayor de la Defensa Nacional. Respecto a los segundos, señala que comprenden el procesamiento de la información relacionada con las actividades de personas, grupos y organizaciones que de cualquier manera afecten o puedan afectar las condiciones del orden público y de la seguridad pública interior y que corresponden ser ejercidas por Carabineros de Chile y por la Policía de Investigaciones de Chile.

Ahora bien, respecto de las formas de intromisión a la privacidad que contempla la Ley de Inteligencia, encontramos su título V, denominado «Los procedimientos especiales de obtención de información», según el cual cuando determinada información resulte ser estrictamente indispensable para el cumplimiento de los objetivos del Sistema de Inteligencia del Estado y no pueda ser obtenida por «fuentes abiertas», se podrán utilizar los procedimientos especiales de obtención de información con el objeto de resguardar la seguridad nacional y proteger a Chile y a su pueblo de las amenazas del terrorismo, el crimen organizado y el narcotráfico.

Los procedimientos especiales de obtención de información señalados por la ley son los siguientes:

- la intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas;
- la intervención de sistemas y redes informáticos;
- la escucha y grabación electrónica, incluyendo la audiovisual; y

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

Ley 20.000, que sustituye la Ley 19.366, que Sanciona el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas (Ley de Drogas)

Esta ley hace alusión expresa a la voz *vigilancia*, refiriéndose a ella en su artículo 23, cuando habla del control y la observación por parte de la autoridad respecto a la circulación de la droga. Sin embargo, al referirse a ella lo hace respecto a la observación física, ya que la vigilancia recae sobre las entregas: los traspasos de las sustancias o drogas estupefacientes o sicotrópicas.

Sin perjuicio de lo anterior, en sus artículos siguientes la ley permite al Juez de Garantía respectivo autorizar la adopción de medidas de retención e incautación de correspondencia, obtención de copias de comunicaciones o transmisiones, interceptación de comunicaciones telefónicas y uso de otros medios técnicos de investigación, pudiéndose aplicar respecto de todos los delitos previstos en esta ley, sin importar su pena. Esta ley va incluso más allá, debido a que permite autorizar la vigilancia incluso sin cumplir con el requisito del artículo 222 del CPP, en cuanto a indicar circunstanciadamente el nombre y dirección del afectado por la medida, siendo suficiente consignar las circunstancias que lo individualizaren o determinaren.

Decreto Ley 211 que Fija Normas para la Defensa de la Libre Competencia (Ley de Libre Competencia)

En conformidad a esta ley, el Fiscal Nacional Económico, con el objeto de promover y defender la libre competencia en los mercados, tendrá entre otras facultades la de solicitar autorización para que Carabineros o la Policía de Investigaciones proceda a entrar a recintos públicos o privados y, si fuere necesario, allanar y descerrajar, registrar e incautar toda clase de objetos y documentos que permitan acreditar la existencia de la infracción, autorizar la interceptación de toda clase de comunicaciones y ordenar a cualquier empresa, que preste servicios de comunicaciones, que facilite copias y registros de las comunicaciones transmitidas o re-

cibidas por ella. Dicha autorización deberá ser solicitada, previa aprobación del Tribunal de Defensa de la Libre Competencia, al Ministro de Corte de Apelaciones correspondiente.

Al revisar el marco normativo del ordenamiento jurídico de Chile es posible notar que existen redundancias, debido a la vaguedad y amplitud de las normas que establecen estas intromisiones a la privacidad. Así, por ejemplo, la Ley de Inteligencia establece formas de obtención de información de fuentes cerradas, las cuales podrían a su vez ser comprendidas dentro de aquellas diligencias establecidas en la Ley de Libre Competencia, la Ley de Drogas y en el CPP. A su vez, la misma Ley de Inteligencia señala que las diligencias que establece sólo pueden ser ejercidas por los funcionarios que sean parte del Sistema de Inteligencia del Estado, imponiendo sanciones penales para quienes las infrinjan. El problema está en que las distintas normas citadas habilitan a funcionarios que podrían no ser parte del Sistema de Inteligencia del Estado, lo que los hace responsables penalmente.

De esta forma, la vaguedad y amplitud permiten que estas normas sean interpretadas de forma que autoricen la recopilación, almacenamiento y eventualmente el análisis de la información obtenida de internet, la cual podría ser utilizada en la búsqueda de sospechosos e incluso vincularlos a casos reales, pudiendo en consecuencia existir un monitoreo sistemático de los usuarios de internet.

Ahora, la pregunta es si efectivamente estos monitoreos sistemáticos en internet son intromisiones que nuestro ordenamiento jurídico contempla y permite. Para responder esto consideramos necesario referirnos a lo que ha señalado recientemente el Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) y, a su vez, a algunas situaciones que han tenido lugar en el último tiempo.

VIGILANCIA EN INTERNET Y EL INFORME DEL ALTO COMISIONADO DE LAS NACIONES UNIDAS PARA LOS DERECHOS HUMANOS

Tal como hemos señalado anteriormente, el derecho a la privacidad no es un derecho absoluto y, en consecuencia, puede ser objeto de restricciones siempre y cuando se respeten ciertos límites (Dulitzky, 2004: 102-103). Así, tanto en la Constitución como en tratados internacionales de derechos humanos, el derecho a la privacidad incluye en su pro-

pio reconocimiento criterios válidos que autorizan que sea restringido legítimamente.[27]

En relación a las restricciones y limitaciones del derecho a la privacidad en el contexto de las nuevas tecnologías, el ACNUDH en su informe *El derecho a la privacidad en la era digital* (2014) se refirió, entre otras cosas, a la situación actual que genera la vigilancia en internet. De ello nos parece necesario remarcar tres de sus declaraciones:

1. *Las medidas de vigilancia no deben injerir arbitraria o ilegalmente en la privacidad, la familia, el domicilio o la correspondencia de un individuo*. Respecto a esto señala que la vigilancia de las comunicaciones electrónicas puede ser una medida necesaria y eficaz para los fines legítimos de las fuerzas del orden o los servicios de inteligencia siempre y cuando se haga en cumplimiento de la ley. Pese a ello, señala que la vigilancia en masa presenta serias dudas respecto a su compatibilidad con los derechos humanos, razón por la cual aborda los siguientes temas:

Injerencias. El ACNUDH se refiere al alcance y el contenido del derecho a la privacidad en relación a que ciertas personas han sugerido que la interceptación o la recopilación de datos acerca de una comunicación difieren del contenido de la comunicación, razón por la cual no constituirían en sí mismas injerencias en la vida privada. Ante esto afirma que la agregación de la información comúnmente conocida como «metadatos» puede incluso dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada. Concluyendo, en consecuencia, que toda captura de datos de las comunicaciones es potencialmente una injerencia en la vida privada (ACNUDH, 2014: 7).

Agrega además que la recopilación y conservación de datos de las comunicaciones equivale a una injerencia en la vida privada, con independencia de si posteriormente se consultan o utilizan esos datos. Incluso la mera posibilidad de que pueda captarse información de las comunicaciones crea una injerencia en la vida privada y puede tener un efecto

27. Así, por ejemplo, el artículo 19 número 5 de la Constitución señala: «El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley».

negativo en otros derechos, como por ejemplo los relativos a la libertad de expresión y de asociación (ACNUDH, 2014: 7).

¿Qué se entiende por «arbitrarias o ilegales»? Respecto a este punto se señala que las injerencias sólo pueden estar establecidas por ley, e incluso cuando esa ley nacional va en contradicción de lo establecido en los tratados de derechos internacionales esa injerencia es ilegal. Luego aborda el tema de las injerencias arbitrarias sosteniendo que cuando los Estados introducen restricciones, éstas deben siempre demostrar que se cumple con los principios generales de legalidad, necesidad y proporcionalidad (ACNUDH: 2014: 8).

Dicho lo anterior, hace referencia a estos principios señalando que toda limitación a los derechos a la privacidad debe estar prevista en la ley, y la ley debe ser lo suficientemente accesible, clara y precisa para que una persona pueda leerla y saber quién está autorizado a realizar actividades de vigilancia de datos y en qué circunstancias. Luego señala que la limitación debe ser necesaria para alcanzar un objetivo legítimo, así como proporcional al objetivo y a su vez debe ser la opción menos perturbadora de las disponibles. Añade que debe demostrarse que la limitación impuesta al derecho tiene posibilidades de alcanzar ese objetivo. Agregando, a su vez, que las limitaciones al derecho a la privacidad no deben «vaciar» el derecho en su esencia y deben ser compatibles con otras normas de derechos humanos, incluida la prohibición de la discriminación. De esta forma, si la limitación no cumple esos criterios sería ilegal y/o arbitraria (ACNUDH: 2014: 9).

El informe sostiene que cuando existen objetivos legítimos y se han establecido las salvaguardias apropiadas, puede permitirse a un Estado realizar actividades de vigilancia; sin embargo, es el gobierno quien debe demostrar que la injerencia es necesaria y proporcional al riesgo concreto que genera. Teniendo esto en consideración, el ACNUDH se refiere a los programas de vigilancia masiva y sostiene que «no es suficiente que las medidas tengan por objeto encontrar determinadas agujas en un pajar; lo importante es el impacto de las medidas en el pajar, en comparación con el riesgo de que se trate; es decir, si la medida es necesaria y proporcionada» (ACNUDH: 2014: 9).

Luego, el ACNUDH analiza la situación del acceso y uso de los datos. Respecto a esto sostiene que recientemente ha existido una creciente colaboración entre los gobiernos con entidades del sector privado. A

raíz de ello algunas empresas, como compañías telefónicas, proveedores de servicios de internet, entre otros, estarían almacenando metadatos acerca de las comunicaciones y la ubicación de sus clientes para que, posteriormente, las fuerzas de orden y los organismos de inteligencia puedan acceder a ellos, sosteniendo que esto no parecería ser necesario ni proporcionado.

Finalmente, el ACNUDH señala que para determinar la proporcionalidad debiera considerarse qué se hace con los «datos a granel» y quién puede acceder a ellos. Considera importante estos factores debido a que muchos marcos nacionales carecen de «limitaciones de uso». Añade que «la inexistencia de limitaciones de uso efectivas se ha exacerbado desde el 11 de septiembre de 2001, y la línea que separa la justicia penal de la protección de la seguridad nacional se ha difuminado significativamente» (ACNUDH: 2014: 10). Sobre esto último afirma que el intercambio resultante entre las fuerzas del orden, los organismos de inteligencia y otros órganos del Estado incrementaría el riesgo de que la vigilancia masiva vulnere la privacidad, toda vez que aun cuando sea necesario el uso de estos datos para un objetivo legítimo, pueden, sin embargo, no serlo para fines distintos no contemplados al momento de su obtención (ACNUDH: 2014: 10).

2. *Protección de la ley*. En este punto señala que el Estado debe asegurarse de que toda injerencia deba estar autorizada por leyes que: a) sean de acceso público; b) contengan disposiciones que garanticen que la obtención, el acceso y la utilización de los datos de las comunicaciones obedezcan a objetivos específicos legítimos; c) sean suficientemente precisas y especifiquen en detalle las circunstancias concretas en que dichas injerencias pueden ser autorizadas, los procedimientos de autorización, las categorías de personas que pueden ser sometidas a vigilancia, el límite de la duración de la vigilancia y los procedimientos para el uso y el almacenamiento de los datos recopilados; y d) proporcionen salvaguardias efectivas contra el uso indebido.

Agrega, además, que en conformidad con las obligaciones internacionales de los Estados, el hecho de que algunos no adopten medidas efectivas para proteger a las personas sujetas a su jurisdicción contra las prácticas ilegales de otros Estados o entidades comerciales, significa la contravención de sus obligaciones en materia de derechos humanos (ACNUDH, 2014: 11).

3. *¿A quién se protege y dónde?* El ACNUDH sostiene en este punto que los Estados no pueden eludir sus responsabilidades en materia de derechos humanos limitándose a mantener esas potestades fuera del alcance de la ley. Lo contrario no sólo supondría socavar la universalidad y la esencia de los derechos protegidos por el derecho internacional de los derechos humanos, sino que también podría crear incentivos estructurales para que los Estados externalicen la vigilancia entre sí (ACNUDH, 2014: 11). Agrega que, en relación a la vigilancia digital, los Estados pueden tener comprometidas sus obligaciones en materia de derechos humanos si la vigilancia digital se realiza en su territorio a personas situadas fuera de su territorio. En este sentido, señala que el principio de no discriminación debe regir por parte del Estado, resguardando a toda persona, sean éstas nacionales o no nacionales, de las vulneraciones al derecho a la privacidad.

SITUACIONES PUNTUALES

EL CASO DEL ESTUDIANTE DE SOCIOLOGÍA DE LA UNIVERSIDAD DE CHILE

El 1 de mayo del año 2014, durante la marcha convocada en Santiago por la Central Unitaria de Trabajadores (CUT) con motivo del Día Internacional del Trabajador, se informó en varios noticiarios del país una agresión a un teniente de Carabineros, quien resulto ser víctima de varios golpes, sufriendo una fractura nasal y la pérdida de una pieza dental. Pasado unos días, los noticieros volvieron a recordar el hecho, esta vez al indicar a un estudiante de sociología de la Universidad de Chile como sospechoso de haber participado de la agresión, quien habría sido detenido. La detención se habría realizado por parte del personal del OS-9 de Carabineros, quienes lo habrían identificado luego de realizar una investigación y revisión de las cámaras de seguridad ubicadas en la calle Brasil con Huérfanos, lugar en donde habría ocurrido el incidente.

La formalización del estudiante se realizó al día siguiente de su detención en el Séptimo Juzgado de Garantía de Santiago por el delito de maltrato de obra en contra de Carabineros. En la ocasión, la Fiscalía Centro Norte de la Región Metropolitana solicitó la prisión preventiva del imputado, mientras que la defensa del estudiante de sociología indicó reiteradamente que él se habría encontrado trabajando, por lo que no

habría asistido a la manifestación. Conocidos los antecedentes, y escuchadas las intervenciones de los abogados, el tribunal resolvió desestimar las pruebas reunidas y las evidencias que inculpaban al estudiante, procediendo en consecuencia a dejarlo en libertad.[28]

Debido a lo anterior, la Fiscalía apeló a la resolución teniendo como principal fundamento el análisis de información en las redes sociales, junto a la fotografía de perfil del estudiante.[29] Llegados los antecedentes a la Corte de Apelaciones de Santiago, ésta decidió revocar la resolución del tribunal de garantía decretando como medidas cautelares la firma mensual y el arraigo nacional del estudiante.[30] Luego de dicha resolución, la investigación prosiguió y no fue sino hasta fines del mes de diciembre de 2014, es decir, siete meses después de su arresto y formalización, que la Fiscalía decidió no perseverar, debido a que no contaba con los antecedentes suficientes para que fuera condenado por el delito que se le acusaba.

Sin perjuicio del relato anterior, resulta relevante en el contexto del presente trabajo lo señalado por la abogada del estudiante, quien advirtió distintas situaciones que le llamaron la atención. En relación a la decisión del tribunal indicó:

> Lo que cuestionamos en la misma audiencia es que este peritaje antropomórfico no es de calidad y de hecho concluye que solamente se pueden evidenciar características físicas similares. Del análisis del mismo peritaje podemos desprender que ni el pelo, ni las cejas, ni el mentón, ni muchas otras características se parecen en absoluto a Bryan.[31]

La misma abogada señaló en otro medio de prensa:

> Uno eventualmente podría discutir que estamos ahí agrediendo o vulnerando la vida privada de Bryan, sin embargo entendemos que también la fotografía es del perfil, el cual es público, la cual desde ahí se

28. Sentencia Séptimo Juzgado de Garantía de Santiago del 20 de mayo de 2014, rol interno O-8316-2014.

29. «Estudiante acusado de agredir a carabinero el 1 de mayo fue formalizado y quedó en libertad», *Radio ADN*, 20 de mayo de 2014, disponible en <http://bit.ly/1KUhYx6>.

30. Sentencia Corte de Apelaciones de Santiago del 28 de mayo de 2014, rol 1510-2014.

31. «Abogada acusó eventual 'lista negra' tras formalización de joven por agresión a policía», *Cooperativa*, 20 de mayo de 2014, disponible en <http://bit.ly/1Mkhyoh>.

> podría extraer. Lo complejo es que, y que también lo hizo ver el magistrado al entregar la resolución, es que *cómo dentro de 6 millones de cuentas de Facebook, de todos los chilenos, se puede determinar que efectivamente Bryan es el que habría participado*. Esa es la duda fundamental. En qué momento se determina si es Bryan quien participa [El énfasis es nuestro].[32]

Lo advertido por la abogada y el juez de garantía permite a lo menos plantearnos la duda respecto a qué medios habría utilizado el Ministerio Público para obtener dicha información. Si consideramos la existencia de la vigilancia en internet, esto comienza a tener sentido.

En la misma nota de prensa anterior hay, además, otro comentario de la abogada que resulta relevante:

> Como bien declaró Bryan en la misma audiencia, y al final a la prensa, nosotros creemos que se puede deber a un hostigamiento policial o a algún tipo de persecución política, aunque desconozco cuáles serían las razones. Entiendo que Bryan también participa activamente en la Federación de Estudiantes de la Universidad de Chile (Fech), se vincula con organizaciones sindicales y a la FEL (Federación de Estudiantes Libertarios).

Finalmente, agrega que: «en ese sentido uno podría entender que habría algún tipo de hostigamiento político al respecto, pero tampoco hay ningún antecedente en concreto que nos permitiría a nosotros manifestar eso […] Según los antecedentes y la forma en la cual se detuvo a Bryan uno podría pensar que sí». De esta forma, las dudas que plantea la abogada y la relación entre la intromisión a la privacidad del estudiante de sociología en el ámbito de la persecución penal nos permiten plantearnos el hecho de que las autoridades sí efectúan vigilancia en internet.

Ahora, si bien lo señalado por la abogada son principalmente suposiciones, resulta relevante considerar el reportaje del diario *La Segunda* al que nos referiremos a continuación, ya que esas suposiciones podrían ser aquí confirmadas.

---

32. «Defensa de estudiante formalizado por ataque a teniente evalúa reclamo en Fiscalía», *BioBio Chile*, 20 de mayo de 2014, disponible en <http://bit.ly/1Hgzgk2>.

EL REPORTAJE DE LA SEGUNDA

En el mes de junio del año 2014, el diario *La Segunda* publicó un reportaje que iniciaba con la siguiente frase: «Hace algunos meses, la PDI y la Fiscalía Occidente investigaban a una banda por robos a cajeros automáticos y tuvieron en Facebook a un gran aliado».[33] El reportaje continuaba señalando algunos ejemplos en los cuales los usuarios habían cometido algunas imprudencias que permitían su vinculación a delitos. Un funcionario entrevistado señalaba:

> La juventud e imprudencia de los implicados los llevó a hacer comentarios en sus perfiles que los vinculaban con los ilícitos, e incluso a publicar fotos «con torres de dinero». Sus nexos en la red también desarmaron sus coartadas, que afirmaban que no se conocían entre sí. En otras imágenes aparecían usando las mismas vestimentas con las que se veían robando en las cámaras de seguridad. Incluso la mesa donde posaban con el dinero fue encontrada en uno de los allanamientos a sus casas. Otro caso ocurrió en Arica, donde el fiscal Mario Carrera logró condena por tráfico contra una mujer, luego de que una madre interceptara el diálogo en Facebook, en el que la hoy condenada ofrecía drogas a su hija.

Así, mediante estos ejemplos se intentaba ilustrar la importancia adquirida por las redes sociales en la persecución penal. El reportaje proseguía señalando que, según cifras de la PDI, desde el año 2012 los requerimientos de información enviados desde Chile a Facebook se habían incrementado de forma progresiva. De modo que si en el año 2012 fueron 295 requerimientos, al año siguiente fue el doble. Incluso hasta mayo del 2014, ya iban en 255. Destacando que nuestro país sería el que más requerimientos formula después de Brasil.

Además se señalaba que hoy ya no sólo existiría un empadronamiento tradicional, realizado por la Policía en terreno, sino que se sumaría ahora el «empadronamiento digital», el cual podría arrojar resultados igualmente valiosos. Estos resultados podrían comprender: «contactos, hábitos, lugares visitados, sitios de trabajo o de estudio. Incluso estados de ánimo: los perfiles públicos *online* que los usuarios

33. «Trabajo policial usa cada vez más los datos de Facebook para atrapar delincuentes», *La Segunda*, 16 de junio de 2014, disponible en <http://bit.ly/1eH6vmT>.

crean en las redes sociales pueden entregar un sinfín de datos vitales para aclarar un caso».

Más adelante en el reportaje, Mauricio Fernández, director de la Unidad Especializada de Lavado de Dinero, Delitos Económicos y Crimen organizado de la Fiscalía Nacional, mencionaba que «a su juicio, las redes ofrecen 'información fresca que en algunos casos puede dar mejores resultados' que los datos tradicionales, como perfiles patrimoniales, comerciales o bancarios». Por su parte, Segundo Mansilla, subcomisario de la Brigada del Cibercrimen de la PDI, agregaba: «es difícil que las redes sociales sirvan para acreditar la autoría de un delito por sí solas, pero sirven para establecer identidades, relaciones». Señalando como ejemplo que «antes era normal que dos sospechosos negaran conocerse. Pero hoy puede haber en Facebook una foto de los dos abrazados tomando cerveza. Y eso es mucho mejor que una declaración».

De esta forma, los antecedentes recién señalados nos permiten sostener que en Chile se realizan intromisiones a la privacidad a través de internet,[34] pero todavía cabe responder a la pregunta: ¿es la vigilancia en internet una intromisión que nuestro ordenamiento jurídico contempla y permite?

VIGILANCIA EN INTERNET EN CHILE: LOS PRINCIPIOS DE LEGALIDAD, NECESIDAD Y PROPORCIONALIDAD

Tal como se ha señalado durante este trabajo, la importancia de la privacidad se remonta a siglos atrás. A lo largo de su historia se ha visto enfrentada a nuevos desafíos; la vigilancia es uno de ellos y no es algo nuevo. Sin embargo, las nuevas tecnologías han permitido la existencia de una vigilancia por internet que resulta preocupante debido a la cantidad de personas que pueden ser sometidas a estas medidas y al uso que se le puede dar a esa información, poniendo en riesgo con ello la privacidad de las personas.

34. Si bien las situaciones antes mencionadas se relacionan principalmente con redes sociales, esto se debe en gran medida a que en la actualidad este tipo de plataformas se caracterizan por permitir a sus usuarios comunicarse, interactuar y participar de forma colaborativa. Por eso redes sociales como Facebook, al ser de las más utilizadas, suelen ser las primeras en aparecer cuando nos referimos a la vigilancia en internet. Sin embargo, este tipo de vigilancia no se limita a este tipo de plataformas, sino que también a otras como Flickr, Google, Yahoo, etcétera.

Así, al referirnos al caso del estudiante de sociología y al reportaje publicado por *La Segunda* podemos constatar que Chile no se encuentra ajeno a estas prácticas. En el caso del estudiante podemos ver cómo la información que el mismo estudiante creó y aportó en el uso de plataformas web, habría sido la principal herramienta para que las autoridades lo sindicaran como sospechoso de un ilícito e iniciar un procedimiento en su contra. Tal como su abogada defensora intuyó, esto podría haber sido posible sólo si se efectuaba un análisis de perfiles de personas junto con sus imágenes, amigos, grupos de interés e incluso sus redes profesionales.

Cabe preguntarse, ¿estas formas de investigación de las policías afectan la privacidad? La respuesta evidentemente es sí. El derecho a la privacidad contempla una expectativa de privacidad que se entiende como la noción subjetiva de una persona de estar apartada de la observación de terceros, pudiendo con ello mantener secretos, comunicarse sin injerencias y controlar su información.

Podemos concluir que el estudiante de sociología sufrió una restricción a su derecho a la privacidad producto de la vigilancia en internet. La pregunta que falta por responder es: ¿es esto una intromisión a la privacidad legal y/o arbitraria en Chile? Para responder esta pregunta, debemos analizar si Chile efectivamente cumple con los principios de legalidad, necesidad y proporcionalidad.

CUMPLIMIENTO DEL PRINCIPIO DE LEGALIDAD

Respecto al principio de legalidad,[35] debemos afirmar que en Chile existen normativas expresas que permiten la intromisión a la privacidad, tal como mencionamos al referirnos al marco legal, que establecen quienes estarían autorizados a realizar tales diligencias, incluso facultando a terceros para realizar ciertos actos de intromisión, como por ejemplo

35. Este principio se encuentra contemplado en el artículo 6 de la Constitución al señalar que «los órganos del Estado deben someter su acción a la Constitución y a las normas dictadas conforme a ella, y garantizar el orden institucional de la República». Por su parte, el artículo 19 número 5 de la Constitución señala expresamente: «El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley». Esto último da cuenta de la manifestación expresa de este principio en nuestra Constitución.

cuando el Código de Procedimiento Penal establece la obligación de los prestadores de servicios de internet de llevar un registro de los números IP de las conexiones que realicen sus usuarios por un plazo no inferior a seis meses. A su vez, las distintas normas establecen para cada caso procedimientos específicos, requisitos y señalan incluso que la información obtenida tendrá una limitación en cuanto a su uso. Así, a primera vista pareciera ser que nuestro país cumple con este principio.

Por otra parte, para el caso de la vigilancia en internet es evidente que ésta puede fácilmente coincidir con varias de las intromisiones señaladas. Al tratarse de datos (como el contenido de mensajes, información personal, imágenes, videos, grabaciones de voz) y metadatos (información descriptiva sobre los datos), éstos pueden ser comprendidos como parte de las comunicaciones.

El problema surge cuando analizamos detenidamente estos principios de acuerdo a lo sostenido por el ACNUDH. De esta forma, podemos afirmar que Chile cumple con que estas leyes: a) sean de acceso público, esto porque se encuentran publicadas en normas legales que pasan por un proceso legislativo y que por ello deben ser publicadas; b) contengan disposiciones que garantizan que la obtención, el acceso y la utilización de los datos de las comunicaciones obedezcan a objetivos específicos y legítimos, esto porque las normas referidas se remiten expresamente a sus objetivos y finalidades; y d) proporcionen salvaguardias efectivas contra el uso indebido, esto porque la ley establece obligaciones y responsabilidades respecto al resguardo y uso de la información obtenida por las medidas de intromisión. Sin embargo, Chile pareciera no cumplir a cabalidad con el punto c), esto es, que estas leyes sean suficientemente precisas y especifiquen en detalle las circunstancias concretas en que dichas injerencias pueden ser autorizadas, los procedimientos de autorización, las categorías de personas que pueden ser sometidas a vigilancia, el límite de la duración de la vigilancia y los procedimientos para el uso y el almacenamiento de los datos recopilados. En ninguno de los cuerpos legales señalados se establece en forma precisa y específica un tipo de intromisión que se refiera a la recolección, interceptación, almacenamiento y análisis masivo con las características de la vigilancia en internet.[36]

36. Si bien Chile contempla la posibilidad de que empresas telefónicas y de telecomunicaciones lleven en carácter de reservado un listado actualizado de los rangos de IP y un

Debido a la naturaleza de esta intromisión tampoco es posible señalar que algún cuerpo legal haya establecido a qué personas se les puede someter a este tipo de vigilancia y a ello hay que agregar que la regla general es que la ley siempre cuando se refiere a estas intromisiones lo hace respecto de ciertas personas que resultarían sospechosas por algún motivo en particular. Sin embargo, en el caso de la vigilancia en internet la vigilancia es efectuada en forma masiva, por lo que son objeto de vigilancia miles o millones de personas por el solo hecho de ser usuarios de internet.

Otro aspecto relevante de esta vigilancia es que ella recopila y almacena toda información de forma sistemática, lo que significa que la vigilancia difícilmente es realizada en forma posterior a un requerimiento, sino que, por el contrario, los análisis se realizan respecto de la información previamente recopilada. Es, por lo tanto, una intromisión constante y un monitoreo sistemático sobre un número indeterminado de personas.

Llegado a este punto cabe recordar la incongruencia normativa existente entre la Ley de Inteligencia y los demás cuerpos normativos reseñados, pues el problema específico que se produce es que las autoridades que no estén amparadas por la Ley de Inteligencia estarían contraviniendo esta normativa. Esta incongruencia finalmente impide saber con claridad quiénes estarían autorizados para efectuar este tipo de vigilancia, con qué objetivos y en qué momento.

A su vez, es necesario tener en cuenta que al referirse estas normas a restricciones de un derecho fundamental, la interpretación que se brinda a este tipo de intromisiones debe ser siempre en forma restrictiva, debiendo escogerse, en consecuencia, la interpretación que resulte menos lesiva, tanto para las personas investigadas como para todos quienes se encuentren bajo vigilancia.

En este orden de ideas podemos concluir que Chile no cumple con

---

registro de los números IP de las conexiones de sus usuarios. La aplicación de esta norma establece en forma específica la intromisión de que se trata, quiénes podrían efectuarla, cuánto sería el tiempo que podrían mantener el registro, quiénes podrían tener acceso a él y la obligación genérica de guardar secreto conforme al inciso final del artículo 182 del Código de Procedimiento Penal. Pese a ello, esta medida no se extiende al registro de todos los datos y metadatos producidos en las comunicaciones que se llevan a efecto en internet.

el principio de legalidad, y en razón de ello cualesquiera de los actos de vigilancia en internet son ilegales.

CUMPLIMIENTO DEL PRINCIPIO DE NECESIDAD

El ACNUDH se refiere al principio de necesidad[37] señalando que si bien las intromisiones a la privacidad pueden tener un objetivo legítimo, no basta con ello para que sean procedentes, sino que requerirá que las medidas además sean necesarias para la obtención de ese fin. Por lo anterior, para el caso en que en Chile existiesen leyes que permitieran la vigilancia en internet, éstas sólo debieran aplicarse cuando sea el único medio para alcanzar ese objetivo legítimo, o en el caso de que existan varios medios de ejecución, se debiera optar por el que fuese menos propenso a vulnerar los derechos humanos. Aún así, el ACNUDH no descarta de forma definitiva la aplicación de este tipo de medidas, sin embargo, éstas requieren un estándar de justificación muy alto por parte de los Estados.

Tal como se desprende del caso del estudiante de sociología, los métodos de investigación no parecieran cumplir con este estándar de necesidad, ya que existen acciones menos lesivas que hubieran permitido a las autoridades obtener resultados en su investigación, incluso más certeros y que como consecuencia podrían haber evitado la detención del estudiante. Por su parte, a la hora de aplicar este tipo de medidas debiera existir una investigación en curso de un delito concreto, para el que, debido a su gravedad y circunstancias específicas, no exista otra forma de obtener la información por medios menos gravosos.

CUMPLIMIENTO DEL PRINCIPIO DE PROPORCIONALIDAD

Respecto al principio de proporcionalidad, si Chile contemplara una ley con medidas de vigilancia en internet, debiera examinar si la limitación o restricción producida a los derechos fundamentales afectados constituye una medida equilibrada entre el beneficio para el bien común que

37. Cabe señalar que los principios de necesidad y proporcionalidad no se encuentran señalados expresamente en la Constitución. Sin perjuicio de ello, nuestra jurisprudencia sí recoge estos principios (Arnold, Martínez y Zúñiga, 2012: 84-104).

se obtiene de la limitación y el perjuicio que genera.[38] En este sentido, se debe considerar por un lado la información obtenida y la gravedad de la intromisión al derecho a la privacidad considerando a su vez los distintos derechos que puedan verse afectados por esta intromisión.

Respecto a esto consideramos importante recordar lo sostenido por el Tribunal Constitucional al pronunciarse respecto al sistema de control que contemplaba el proyecto de ley en contra de la pornografía infantil, señalando:

> Que, sin reparar que se impone un sistema de control cuyo peso recae en entidades privadas ajenas a lo policial, el proyecto al impedir que se produzcan filtraciones o se trafique con la información contenida en dichos registros ad hoc, personalísima y valiosa, establece un deber de reserva, que resulta insuficiente para resguardar el derecho de que se trata.[39]

En dicha sentencia se hablaba del registro que los administradores de cibercafés debían llevar respecto de sus usuarios (lo cual despertaba dudas respecto al control del uso de la información). Hoy en día la situación es muy similar, sólo que ya no son los administradores de cibercafés quienes hacen el registro, sino las empresas propietarias de las plataformas web, y ya no son los usuarios de los cibercafés sino que ahora son todos los usuarios de las plataformas de esas empresas, que hoy por hoy resultamos ser todos quienes tenemos cuentas en Google, Facebook, Yahoo, etcétera.

Si ya se tenía dudas de la capacidad de control de la información por parte de los administradores de cibercafés, el problema es mayor si se

38. Nos referimos al principio de proporcionalidad en sentido estricto o a la regla de ponderación. Al respecto Hernán Fuentes Cubillos nos entrega una definición: «la proporcionalidad en sentido estricto, también denominado mandato de ponderación, consiste en 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, 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» (Fuentes Cubillos, 2008: 27). Lo advertimos porque, en general, el test de proporcionalidad considera el análisis de la idoneidad, necesidad y proporcionalidad en sentido estricto (Covarrubias Cuevas, 2014: 164-165).

39. Sentencia del Tribunal Constitucional, rol 1894-11, considerando vigésimo cuarto.

trata de controlar el uso de esta información por partes de esas grandes empresas. Además, pese a las reservas legales que puedan existir en nuestra legislación, éstas podrían ser fácilmente eludidas al ser aplicadas a personas naturales o jurídicas sujetas a jurisdicciones diversas.

En la actualidad existen monitoreos sistemáticos que los Estados como Chile están utilizando y que tienen como consecuencia que las personas se sientan observadas constantemente. Lo que afecta el derecho de privacidad en su esencia, ya que en la práctica en internet no existiría privacidad, y esto finalmente termina afectando otros derechos fundamentales relacionados, como por ejemplo el derecho a la libertad de expresión.[40]

En este sentido, la relatora especial para la Libertad de Expresión, Catalina Botero, señaló en su informe *Libertad de expresión e internet* (cf. CIDH, 2014) que se podían desprender dos tipos de restricciones, a saber:

- Restricciones directas. Como, por ejemplo, que el derecho de libertad de expresión no se podría ejercer de manera anónima como consecuencia de la actividad de vigilancia.
- Restricciones indirectas. La sola existencia de programas de vigilancia masiva de datos produce una limitación indirecta que en consecuencia tiene un efecto inhibidor sobre el ejercicio de la libertad de expresión. Agrega que la afectación de la privacidad de las comunicaciones volvería a las personas cautelosas de lo que dicen y a raíz de ello, también las volvería cautelosas de lo que hacen. De modo que esto no haría más que instalar el temor y la inhibición como parte de la cultura política, obligando así a las personas a tomar precauciones para comunicarse entre ellas (CIDH, 2014: 173).

40. Es relevante mencionar lo señalado por el ACNUDH, quien destacó en su informe la importancia de este derecho en relación a otras garantías, señalando: «Aunque el mandato del presente informe se centró en el derecho a la privacidad, cabe subrayar que otros derechos también pueden verse afectados por la vigilancia en masa, la interceptación de las comunicaciones digitales y la recopilación de datos personales, por ejemplo el derecho a la libertad de opinión y de expresión, y a buscar, recibir y difundir información; el derecho a la libertad de reunión y de asociación pacíficas; y el derecho a la vida familiar. Todos esos derechos están estrechamente vinculados con el derecho a la privacidad y, cada vez más, se ejercen a través de los medios digitales» (ACNUDH, 2014: 6).

La relatora Catalina Botero indicó además que los principales afectados con estas medidas serían aquellos que sostienen las posiciones menos populares, o los miembros de las minorías políticas, raciales o religiosas, agregando que usualmente son ilegítimamente calificados de «terroristas», lo que facilitaría su persecución y con ello que sean objeto de vigilancia y seguimiento sin controles adecuados. Razón por la que declara: «Una sociedad democrática exige que los individuos puedan comunicarse sin interferencias indebidas, lo que requiere que sus comunicaciones sean privadas y seguras» (CIDH, 2014: 173). Si consideramos las actividades que realizaba el estudiante de sociología y las posibilidades que existen de seguir cada una de las actividades y expresiones de las personas por internet, esto indudablemente genera que las personas se sientan inseguras y teman a la hora expresarse en internet, condicionando su forma de actuar.

Chile no cumple con los principios de legalidad, de necesidad ni con el de proporcionalidad. Incumple con su obligación de respetar, garantizar y hacer efectivos los derechos internacionales de derechos humanos, por varios motivos: i) por recibir reportes de información solicitados a empresas de comunicaciones que tendrían programas de vigilancia en internet; ii) por incurrir en injerencias arbitrarias e ilegales, producto de no respetar los estándares mínimos de legalidad, necesidad y proporcionalidad respecto a las medidas de vigilancia en internet que en la actualidad se emplean al requerir de las empresas la entrega de la información; y iii) por no velar por el respeto y protección de los derechos de privacidad, así como también los de otros derechos que pueden ser afectados, como es el caso de la libertad de expresión.

De lo anterior se desprende que si nuestro país decidiese efectuar vigilancia en internet debe adecuar su legislación interna de tal forma que se establezcan expresamente las situaciones, las características, la duración, los procedimientos, quiénes estarían autorizados, los controles efectivos respecto del uso de la información obtenida, entre otros factores que habilitarían la aplicación de estas medidas, debiendo además justificar su necesidad y su proporcionalidad.

CONCLUSIONES

1. El derecho a la privacidad es un derecho que ha ido evolucionando con el tiempo, debido a que se encuentra estrechamente ligado a las condiciones socioculturales existentes en un lugar y tiempo determinados.
2. Pese a la dificultad que existe a la hora de dar un concepto del derecho a la privacidad, lo importante es comprender que el alcance y contenido de este derecho debe resguardar la expectativa de privacidad de las personas.
3. El surgimiento de la web 2.0 ha tenido como una de sus consecuencias el que la privacidad se haya visto en peligro debido a la cantidad y la calidad de la información que estas plataformas pueden obtener debido al contenido que los mismos usuarios generan.
4. Lo anterior ha significado que en la actualidad existan programas de vigilancia en internet capaces de obtener información detallada sobre las vidas, secretos, orientación sexual, identidad, ideología, y un sinfín de información, de la cual incluso los mismos titulares no son conscientes.
5. Si bien se ha reconocido que estos programas de vigilancia en internet pueden ayudar en la consecución de objetivos legítimos, como por ejemplo combatir el terrorismo, el narcotráfico, el crimen organizado, la pornografía infantil, la defensa de la nación u otros, esto no impide que los Estados deban aplicar estas medidas de forma restringida, toda vez que atendida su naturaleza afectan derechos fundamentales.
6. Para que la vigilancia en internet pueda ser entendida como una intromisión legítima es necesario que los Estados cumplan con el principio de legalidad, necesidad y proporcionalidad.
7. En el caso de Chile, no existe norma legal que regule la vigilancia en internet, ni defina qué procedimientos se deben seguir, con qué fines podría ser utilizada, ni qué formas de control existirían.
8. La amplitud de las normativas intrusivas actuales puede crear la falsa imagen, entre los agentes relacionados con la justicia, de que

se encuentran facultados para implementar vigilancia en internet, sin embargo estas normas al restringir derechos fundamentales deben siempre interpretarse restrictivamente.

9. La persecución penal de un estudiante de sociología junto al reportaje efectuado a funcionarios policiales son una muestra de que en Chile efectivamente se implementa la vigilancia en internet.

10. Se desprende de lo anterior que Chile vulnera el derecho a privacidad al no cumplir con los principios de legalidad, necesidad y proporcionalidad en relación a la vigilancia en internet.

11. La vulneración que produce la vigilancia en internet, a su vez, afecta a otros derechos relacionados a la privacidad. Al afectar la libertad de expresión produce dos tipos de restricciones: i) una restricción directa, la cual implicaría que la libertad de expresión no se podría ejercer de manera anónima; y ii) una restricción indirecta, toda vez que la sola existencia de programas de vigilancia masiva de datos tiene un efecto inhibitorio en las personas, quienes no se sentirían seguras de expresarse libremente.

12. Si Chile requiere incorporar la vigilancia en internet para cumplir con sus objetivos legítimos, deberá adecuar su legislación interna, cumpliendo así con los principios de legalidad, necesidad y proporcionalidad de tal forma que se resguarden los derechos de las personas.

13. Finalmente, Chile debe tomar una postura firme respecto a las revelaciones de programas de vigilancia en internet, ya que afectan gravemente derechos como la privacidad y la libertad de expresión, siendo, hasta el momento, inexistentes los controles que resguardan efectivamente la privacidad en internet, sobre todo considerando que muchas de las actividades de vigilancia son efectuadas por entidades privadas internacionales que difícilmente pueden ser controladas.

REFERENCIAS

Anguita, Pedro (2006). «Jurisprudencia constitucional sobre el derecho a la propia imagen y la vida privada en Chile (1981-2004): un intento

de sistematización». En Felipe González (ed.), *Libertad de expresión en Chile* (pp. 319-521). Santiago: Facultad de Derecho, Universidad Diego Portales.

Álvarez Valenzuela, Daniel (2013). «Vida privada en Chile». Centro de Estudios en Derecho Informático de la Universidad de Chile, 30 de enero. Disponible en <http://bit.ly/1KUDMZv>.

ACNUDH, Alto Comisionado de las Naciones Unidas para los Derechos Humanos (2014). *El derecho a la privacidad en la era digital*. Disponible en <http://bit.ly/1HpMZlr>.

Arnold, Rainer, José Martínez Estay y Francisco Zúñiga Urbina (2012). «El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional». *Estudios Constitucionales*, 10 (1): 65-116. Disponible en <http://bit.ly/1RoquIK>.

Castells, Manuel (2009) *Communication and Power*. Oxford: Oxford University Press.

Cedric Laurant (2012). *Guía de privacidad para hispanohablantes* 2012. Disponible en <http://bit.ly/1KgeUsj>.

Clarke, Roger (1994). «Dataveillance: Delivering 1984». En Lelia Green y Roger Guinery (eds.), *Framing technology: Society, choice and change* (pp. 117-130). Sydney: Allen & Unwin.

CIDH, Comisión Interamericana de Derechos Humanos (2014). *Libertad de expresión e Internet*. Oficina de la Relatoría Especial para la Libertad de Expresión. Disponible en <http://bit.ly/1Hk9NX4>.

Corral, Hernán (2001). «El respeto y protección de la vida privada en la Constitución de 1980». En Enrique Navarro (ed.), *Veinte años de la Constitución Chilena,* 1981-2001 (pp. 199-224). Santiago: ConoSur.

Covarrubias Cuevas, Ignacio (2014) «¿Emplea el Tribunal Constitucional el test de proporcionalidad?» *Estudios Constitucionales*, 12 (1): 163-237. Disponible en <http://bit.ly/1RJnE10>.

Dulitzky, Ariel E. (2004). «Alcance de las obligaciones internacionales de los derechos humanos». En Claudia Martin, Diego Rodríguez-Pinzón y José A. Guevara B. (eds.), *Derecho internacional de los derechos humanos* (pp. 79-117). México: Universidad Iberoamericana, Academia de Derechos Humanos y Derecho Internacional Humanitario, Washington College of Law, American University y Districuciones Fontamara. Disponible en <http://bit.ly/1HkcBDr>.

Figueroa, Rodolfo (2013). «El derecho a la privacidad en la jurisdic-

ción de protección». *Revista Chilena de Derecho*, 40 (3): 859-889. Disponible en <http://bit.ly/1MfE2Sh>

Fuchs, Christian (2011) «New media, web 2.0 and surveillance». *Sociology Compass*, 5 (2): 134-147. Disponible en <http://bit.ly/1NYJxUB>.

Gómez, Gastón (2005). *Derechos fundamentales y recursos de protección*. Santiago: Ediciones Universidad Diego Portales.

Greenwald, Glenn (2014). *Snowden: Sin un lugar donde esconderse*. Trad. Joan Soler Chic. Santiago: Ediciones B.

Herrán, Ana (2002). «El derecho a la intimidad en la Nueva Ley Orgánica de Protección de Datos Personales». Madrid: Dykinson.

Jijena Leiva, Renato (2015). «Privacidad, internet y derecho: Un desafío de cara al siglo XXI en el marco de la globalización». Disponible en <http://bit.ly/1VifoGf>.

Michael, James (1994). *Privacy and human rights: An international and comparative study, with special seference to developments in information technology*. París: Unesco.

Nogueira Alcalá, Humberto (2007). «Los derechos contenidos en tratados de derechos humanos como parte del parámetro de control de constitucionalidad: la sentencia rol 786-2007 del Tribunal Constitucional». *Estudios Constitucionales*, 5 (2): 457-466. Disponible <http://bit.ly/1Ib41Ex>.

O'Reilly, Tim (2007). «What is web 2.0: Design patterns and business models for the next generation of software». *Communications & Strategies*, (1): 17-37. Disponible en <http://bit.ly/1dQl32C>.

Rodríguez Pinto, María Sara (1999). «Protección de la vida privada: Líneas jurisprudenciales». *Revista Chilena de Derecho*, 26 (3): 719-744. Disponible para descarga directa en <http://bit.ly/1g1i7Cc>.

Saldaña, María Nieves (2011). «El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego». *Teoría y Realidad Constitucional*, (28): 279-372. Disponible en <http://bit.ly/1GyCRGr>.

Senso, José A. y Antonio de la Rosa (2003). «El concepto de metadato. Algo más que descripción de recursos electrónicos». *Ciência da Informação*, 32 (2): 95-106. Disponible en <http://bit.ly/1HineVc>.

Tapia, Mauricio (2008). «Fronteras de la vida privada en el derecho chileno». *Revista Chilena de Derecho Privado*, (11): 117-144.

Vial, Tomás (2000). «Hacia la construcción de un concepto constitu-

cional del derecho a la vida privada». *Persona y Sociedad*, 14 (3): 47-68.

Warren, Samuel y Louis Brandeis (1995). *El derecho a la intimidad*. Trad. Benigno Pendas y Pilar Baselga. Madrid: Civitas.

SOBRE EL AUTOR

Danny Rayman Labrín es abogado. Licenciado en Ciencias Jurídicas y Sociales de la Universidad Diego Portales. Su correo electrónico es <danny.rayman@gmail.com>. Su dirección postal es Cerro los Azules, 637, Las Condes, Región Metropolitana.

Este trabajo fue recibido el 21 de enero de 2015 y aprobado el 12 de junio de 2015.