Derecho PUCP
ISSN: 0251-3420
ISSN: 2305-2546
revistaderechopucp@pucp.edu.pe
Pontificia Universidad Católica del Perú
Perú

Álvarez Valenzuela, Daniel
Algunos aspectos jurídicos del cifrado de comunicaciones
Derecho PUCP, núm. 83, 2019, pp. 241-264
Pontificia Universidad Católica del Perú
Perú

DOI: https://doi.org/10.18800/derechopucp.201902.008

https://doi.org/10.18800/derechopucp.201902.008

DERECHO PUCP
N° 83, 2019
diciembre-mayo
pp. 241-262
REVISTA DE LA FACULTAD DE DERECHO

Algunos aspectos jurídicos del cifrado de comunicaciones

Some Legal Aspects of Encryption of Communications

DANIEL ÁLVAREZ VALENZUELA*
Universidad de Chile (Chile)

Resumen: Este es un trabajo que explora algunas de las consideraciones jurídicas más relevantes sobre la relación entre cifrado de comunicaciones y ciertos derechos constitucionales, con enfoque en el derecho chileno. Sostenemos que existe una tensión no resuelta en el rol que ejerce el uso de herramientas de cifrado de comunicaciones respecto del ejercicio de esos derechos fundamentales y la seguridad pública. Para ello, luego de introducir brevemente el concepto de cifrado o encriptación, revisamos las bases del debate regulatorio en Estados Unidos, contenido esencialmente en sus reglas sobre inteligencia y sobre control de exportaciones de herramientas de cifrado, y repasamos sintéticamente el debate constitucional norteamericano. Respecto de la Unión Europea, identificamos los principales elementos jurídicos y políticos que están influyendo en el debate prerregulatorio comunitario. Enseguida, se caracterizan los principales aspectos jurídicos involucrados en el uso de herramientas de cifrado.

Palabras clave: encriptación, privacidad, seguridad pública, Chile

Abstract: This work explores some of the most relevant legal considerations on the relationship between encryption of private communications and some constitutional rights, with a focus on Chilean law. We maintain that there is an unresolved tension in the role of the use of communications encryption tools with respect to the exercise of these fundamental rights and public security. To do this, after briefly introducing the concept of encryption, we review the bases of the regulatory debate in the United States, essentially contained in its rules on intelligence and export control of encryption tools, and synthetically review the American constitutional debate. Regarding the European Union, we identify the main legal and political elements that are influencing the community's pre-regulatory debate. Next, the main legal aspects involved in the use of encryption tools are characterized.

***Key words*:** encryption, privacy, public security, Chile

* Abogado, licenciado en Ciencias Jurídicas y Sociales, diplomado en Derecho Informático y magíster en Derecho con mención en Derecho Público, todos por la Universidad de Chile. Académico del Departamento de Derecho Comercial de la Facultad de Derecho, Universidad de Chile. Coordinador Académico del Centro de Estudios en Derecho Informático de la misma facultad y editor general de la *Revista Chilena de Derecho y Tecnología*. El presente artículo forma parte de la investigación doctoral que lleva a cabo el autor en la Universidad de Chile, cuyo título es «La tensión entre seguridad pública y privacidad: el caso del cifrado de comunicaciones».
Código ORCID: 0000-0002-9172-7736. Correo electrónico: dalvarez@derecho.uchile.cl

CONTENIDO: I. INTRODUCCIÓN.– II. LA REGULACIÓN DEL CIFRADO EN ESTADOS UNIDOS.– III. EL DEBATE (PRE)REGULATORIO EN LA UNIÓN EUROPEA.– IV. ASPECTOS JURÍDICOS DEL CIFRADO.– V. LA (NO)REGULACIÓN DEL CIFRADO EN CHILE.– V.1. LA PROTECCIÓN DE LA PRIVACIDAD EN EL DERECHO CONSTITUCIONAL CHILENO.– V.2. EL CONCEPTO DE SEGURIDAD PÚBLICA EN EL DERECHO CONSTITUCIONAL CHILENO.– VI. ¿CÓMO SE RESUELVE ESTA TENSIÓN?.– VII. CONCLUSIONES.

I. INTRODUCCIÓN

El desarrollo y masificación de las tecnologías digitales ha transformado de manera radical la forma en que las personas vivimos en sociedad. Nuestras relaciones personales y profesionales, nuestra actividad económica, comercial e incluso política están en buena medida intermediadas por sistemas informáticos, redes de telecomunicaciones y dispositivos digitales de las más diversas características. La denominada sociedad de la información —que se caracteriza por la disponibilidad, en tiempo real, de ingentes cantidades de información al alcance de cualquier persona con acceso a una red— ha significado un cambio de paradigma social, cultural y económico, mayor incluso que la revolución industrial (Castells, 1999).

En este contexto, el surgimiento de Internet —a principios de la década de los ochenta y su masificación a partir del año 1994, con la invención de la *world wide web*— revolucionó no solo el mundo de las tecnologías, sino que se constituyó en un nuevo espacio de relaciones sociales. Según Castells, la red no es solo una tecnología, es mucho más, «[e]s un medio de comunicación, de interacción y de organización social» (s.f.).

En el ámbito de las relaciones personales, en no más de dos décadas pasamos de utilizar medios de comunicación esencialmente analógicos —como la correspondencia postal o el teléfono— a emplear una amplia gama de medios basados en Internet —como el correo electrónico, la mensajería instantánea, las redes sociales— y aplicaciones como WhatsApp, Telegram o Signal se han vuelto enormemente populares. No obstante la gran utilidad de estos nuevos medios de comunicación personal, ellos representan, al mismo tiempo, nuevas amenazas al ejercicio de derechos fundamentales como la vida privada o la inviolabilidad de las comunicaciones privadas. Las revelaciones de Edward Snowden sobre sistemas de vigilancia masiva de las comunicaciones en Internet dieron cuenta de la vulnerabilidad de este tipo de plataformas (Mattelart & Vitalis, 2015). Surgió entonces, para algunos, la necesidad de utilizar herramientas de encriptación o cifrado[1] de comunicaciones que

1 Si bien en el lenguaje técnico existen sutiles diferencias entre los términos «cifrado» y «encriptación», en el lenguaje común se utilizan indistintamente como sinónimos y así serán consideradas en este trabajo.

permiten agregar una capa de inviolabilidad técnica no normativa a los actos comunicativos intermediados por tecnologías. El uso de cifrado puede ser leído incluso como una forma de reacción política frente al Estado vigilante. Así sostiene, por ejemplo, Assange al señalar que la «criptografía es la forma más acabada de acción directa no violenta» (Assange, 2013, p. 26).

En términos simplificados, el cifrado de comunicaciones consiste en la utilización de un algoritmo matemático que «envuelve» un mensaje de manera que solo el receptor legítimo pueda abrirlo y hacerse de su contenido, mediante la utilización de una llave o clave única que «desenvuelve» el mensaje. El propósito del cifrado es hacer ininteligible un mensaje a los ojos de un tercero ajeno a la comunicación[2].

La criptografía ha sido usada casi simultáneamente desde el desarrollo avanzado del lenguaje escrito (Singh, 2000) y tradicionalmente jugó un rol fundamental en la protección de las comunicaciones oficiales de los Estados, de los gobernantes y, principalmente, de las instituciones militares. Fueron precisamente los grandes conflictos bélicos del siglo XX, los que permitieron el desarrollo de los principales avances en la criptografía moderna, especialmente a partir de la invención de los métodos de computación electrónica —que facilitaron el procesamiento de grandes volúmenes de información[3]— y el desarrollo de un ámbito específico de las matemáticas: las teorías de la información de Claude Elwood Shannon, quien es considerado el padre de la criptografía moderna (Granados, 2006, p. 6; Singh, 2000). En América Latina existen antecedentes del uso de herramientas de cifrado de comunicaciones desde la Conquista y su uso se intensificó durante la Colonia y los procesos independentistas (Galende, 2000). En el caso de Chile, no existen antecedentes ni estudios públicos que den cuenta del uso de este tipo de herramientas en nuestra historia.

II. LA REGULACIÓN DEL CIFRADO EN ESTADOS UNIDOS

Atendiendo a la fuerte vinculación de la criptografía con el mundo militar y las actividades de inteligencia, los primeros desarrollos normativos relativos al cifrado de comunicaciones forman parte de las reglas sobre seguridad nacional, especialmente en países como Estados Unidos, Reino Unido y Alemania, en los que se recogió la extensa experiencia acumulada durante la II Guerra Mundial, que fue extremadamente provechosa durante la Guerra Fría. En el caso de

2 Desde un punto de vista etimológico, la expresión «criptografía» proviene de la conjunción de las expresiones griegas kriptos (oculto) y graphos (escritura), por lo que significaría ocultar la escritura (Granados, 2006, p. 6).

3 Alan Turing, uno de los inventores de la computación, fue al mismo tiempo uno de los responsables de la desencriptación del cifrado que protegía las comunicaciones alemanas durante la II Guerra Mundial, lo que habría precipitado el término del conflicto (Singh, 2000).

Estados Unidos, la National Security Agency (NSA) es el organismo del sistema de inteligencia norteamericano encargado de la denominada inteligencia de comunicaciones[4], quedando bajo su mando técnico y operacional todas las actividades de recojo, procesamiento y análisis de las comunicaciones telefónicas y electrónicas de terceros países y la protección de las redes propias y de sus aliados (Thiber, 11 de noviembre de 2013). Creada secretamente en el año 1952 por el presidente Harry Truman, a través de un memorándum (Memorandum for the Secretary of State and the Secretary of Defense), su existencia fue develada públicamente recién en el año 1972, ante la Comisión Investigadora del Senado sobre Inteligencia de ese país (Mattelart & Vitalis, 2015, p. 89). Las operaciones de la NSA están parcialmente reguladas en el Foreign Intelligence Surveillance Act de 1978 (FISA).

En el ejercicio de sus atribuciones legales, la NSA cumplió un rol fundamental tanto en el desarrollo de la criptografía contemporánea como en la restricción de la circulación de información sobre la misma. Entre 1950 y mediados de la década de los ochenta, la NSA controló y limitó la publicación o divulgación de información relativa a la encriptación, y cualquier escrito o investigación sobre el tema debía ser previamente censado por esa agencia, estableciéndose el denominado «criptosecretismo»[5]. Posteriormente, con ocasión del surgimiento de tecnologías de cifrado civiles, estas prácticas dieron origen a las denominadas «criptoguerras» que enfrentaron a las autoridades políticas y del sistema de inteligencia de Estados Unidos con la comunidad científica y tecnológica vinculadas al desarrollo de sistemas de cifrado (Levy, 2002). Asimismo, la NSA contaba con la autoridad legal para declarar secreta cualquier patente relacionada con criptografía y la revelación no autorizada de información sobre sus operaciones, desarrollos e investigaciones podía ser constitutiva del delito de traición (Levy, 2002).

Si bien no existe norma expresa en el derecho norteamericano que prohíba el desarrollo o uso de herramientas de encriptación, la exportación de estas —o de aplicaciones que utilicen alguna forma o tipo de tecnología de cifrado— estuvo sujeta a las normas federales Export Administration Regulations (EAR). En un primer momento y hasta comienzos de este siglo, estas regulaciones establecían un régimen de prohibición de la exportación de los mecanismos de cifrado fuerte[6]. A partir de 1999

4 La inteligencia de comunicaciones (COMINT) es un método de obtención de información de inteligencia mediante la escucha o interceptación de Comunicaciones y es una de las dos variables —junto a la inteligencia electrónica (ELINT)— que conforman la denominada Inteligencia de Señales (SIGINT) (Sainz, 1991).

5 La obra del periodista David Khan, The Codebreakers, quizás la mayor investigación histórica sobre encriptación, fue sometida a censura previa por la NSA, al tratar sobre asuntos que podían afectar la seguridad nacional (Velasco, 20 de mayo de 2014).

6 La diferenciación entre mecanismos de cifrado fuerte o débiles dice relación con la capacidad del mecanismo de resistir de mejor o peor manera los intentos de descifrar el código sin utilizar la clave legítima.

(Swire, 2012, p. 202), pasaron a una modalidad de control a través de prohibiciones de exportación a ciertos países, obligaciones de registros y la concesión de licencias para la exportación de este tipo de productos. Dicho sistema de control es administrado por la Oficina de Seguridad e Industria del Departamento de Comercio de Estados Unidos.

Por su parte, tanto el Capítulo 119 de la Parte I del Título 18 del U.S. Code (Wire and Electronic Communications Interception and Interception of Oral Communications) como las disposiciones del USA PATRIOT Act de 2001 establecen extensas regulaciones sobre la interceptación de comunicaciones físicas, electrónicas o digitales, aplicables a la investigación de crímenes o de actividades terroristas, respectivamente. Sin embargo, dichas normas no establecen reglas específicas sobre el cifrado, lo que ha permitido —en la práctica— que, si una agencia de investigación en el ejercicio de sus atribuciones se enfrenta a este tipo de tecnologías al momento de llevar a cabo una interceptación, se encontraría facultada para descifrarlas, usando los medios técnicos y humanos de que disponga[7].

Con todo, a partir de la incorporación por defecto de tecnologías de cifrado punto a punto[8] en teléfonos y dispositivos móviles de última generación, se ha incrementado el número de casos donde la autoridad judicial o policial no puede acceder a la información encriptada, por la imposibilidad técnica que suponen las potentes herramientas de cifrado utilizadas[9]. A nivel constitucional, existe cierto nivel de acuerdo en la doctrina (Post, 2000; McClure, 2000) y en la jurisprudencia norteamericana (*Bernstein v. United States*) en considerar que el cifrado —en tanto expresión escrita de un lenguaje específico— se encuentra bajo el amparo de la Primera Enmienda sobre libertad de expresión, de manera tal que el derecho a desarrollar tecnologías de cifrado, su publicación y eventual distribución no pueden ser restringidos por decisiones gubernamentales. No existe tal nivel de acuerdo en la doctrina (Calo, 2016) ni hay jurisprudencia que constituya precedente respecto a la protección constitucional del uso de herramientas de cifrado como

7 Es el caso, por ejemplo, del debate judicial y comunicacional que se generó a partir de la solicitud del FBI a Apple de desencriptar el iPhone de uno de los responsables de la masacre de San Bernardino, cuyo contenido estaba protegido por el sistema de encriptación de discos de OSX. Ante la negativa de Apple, el FBI contrató los servicios de una empresa israelita de seguridad, quienes lograron acceder a la información a través de mecanismos que no han sido develados públicamente (Israeli Firms, 23 de marzo de 2016).

8 El cifrado punto a punto consiste en una herramienta de encriptación que funciona en el dispositivo de cada usuario final que cifra todos los mensajes salientes con una llave única que solo el receptor legítimo de la comunicación puede descifrar. Esta modalidad impide que el prestador de servicios de comunicaciones tenga acceso al contenido de la comunicación, porque no tiene las llaves necesarias para descifrar el tráfico que se genera.

9 A octubre de 2017, según el director del FBI, Christopher Wray, más de siete mil dispositivos móviles han quedado fuera de la acción de esta agencia gubernamental como consecuencia de los sistemas de cifrado automatizado que ofrecen a sus clientes empresas como Apple y Google, entre otras (Abel, 24 de octubre de 2017).

objeto de la Cuarta Enmienda[10] de la Constitución de Estados Unidos de 1791, que reconoce el derecho de las personas, sus hogares, documentos y pertenencias frente a intromisiones, allanamientos o registros arbitrarios de la autoridad. La Cuarta Enmienda protege implícitamente el derecho individual a la privacidad limitando las potestades investigadoras del Estado, quien deberá contar con una orden judicial y causa probable para justificar la intromisión de la autoridad en la legítima expectativa de privacidad de una persona (Gonzalez, 2019).

Por una parte, autores como Amitai Etzioni sostienen —desde una perspectiva liberal comunitaria— que la norma constitucional fija las reglas necesarias para que una corte determine, en el caso concreto, qué bien será objeto de protección especial en el caso de la tensión entre privacidad y seguridad nacional, identificando, al menos, cuatro criterios distintos que permitirían descartar que el cifrado esté protegido por dicha garantía constitucional: (a) autorizaciones judiciales expedidas conforme a la ley; (b) daños inherentes que ocasionaría el cifrado; (c) el interés público en casos especialmente graves; y (d) obstrucción a la justicia (Etzioni, 2015). En la posición contraria, Cindy Cohn (2014) afirma que el uso de herramientas de cifrado, para proteger comunicaciones y personas así como también como mecanismo para encriptar archivos de información (*data encryption*), además de estar protegido por la Primera Enmienda, puede entenderse comprendido en la garantía de la Cuarta Enmienda. Como ya se ha indicado, la Cuarta Enmienda no autoriza al gobierno a allanar o ingresar a un hogar para acceder a documentos personales sin antes probar que se cumplen los requisitos de «causa probable», debiendo aplicarse el mismo estándar en el caso de las comunicaciones digitales sin necesidad previa de desencriptar el contenido de estas. El rol que jugaría el cifrado en este debate no es claro para la doctrina, toda vez que sin perjuicio de existir una orden judicial, dictada conforme a la regla constitucional, no implica necesariamente la orden de descifrar un determinado contenido, a menos que las agencias estatales usen herramientas de *hacking* que, aprovechándose de alguna vulnerabilidad de los dispositivos o el *software*, pueden acceder a esos contenidos (Kerr & Schneier, 2018). El uso de este tipo de técnicas plantea importantes discusiones éticas y de políticas públicas (Gonzalez, 2019).

Como bien apunta Gonzalez, el debate sobre los efectos de la Cuarta Enmienda en el uso de herramientas de cifrado tendría más efecto en el caso que el Congreso de Estados Unidos aprobare una ley que obligara a

10 «El derecho del pueblo a la seguridad de sus personas, hogares, documentos y pertenencias frente a allanamientos y registros arbitrarios será inviolable, y no se expedirá ningún mandamiento, sino en virtud de causa probable, apoyado en juramento o promesa, que describa el lugar que ha de ser registrado y las personas o cosas que han de ser detenidas o incautadas» (IV Enmienda, Constitución de Estados Unidos de Norteamérica de 1791).

las compañías proveedores de sistemas de cifrado a incorporar «puertas traseras»[11], ya que una regla de esa naturaleza podría ser declarada inconstitucional por afectación de la privacidad (Gonzalez, 2019).

En el contexto de la lucha contra el terrorismo en Estados Unidos, el debate se ha concentrado en determinar si el cifrado de comunicaciones puede ser absoluto, esto es, que nadie que no sea el titular o el receptor de una comunicación privada pueda acceder a ella o, si es necesario que se establezcan reglas que permitan a las autoridades policiales y o judiciales «romper» los mecanismos de encriptación, a través del establecimiento de obligaciones de colaboración a los usuarios de estos mecanismos o a las empresas que proveen algún tipo de producto o servicio de telecomunicaciones, como por ejemplo, el establecimiento de «puertas traseras» que permitan saltarse los mecanismos de encriptación (Kerr & Schneier, 2018).

III. EL DEBATE (PRE)REGULATORIO EN LA UNIÓN EUROPEA

En el caso de la Unión Europea, desde la década de las noventa, el cifrado se ha convertido en un componente esencial de la apertura social y de mercados que ha llevado a cabo ese bloque económico y político. El uso de herramientas de cifrado ha elevado los niveles de protección de todo tipo de transacciones o intercambios de información, desde las transacciones financieras hasta el tratamiento de información clínica confidencial (Koomen, 2019). En el caso de Alemania, desde el año 1999 se han implementado instrumentos de política pública para desarrollar, apoyar, y fomentar el uso no regulado de tecnologías de encriptación. Como señalan Sven Herpig y Stefan Heumann, en el año 2014, el gobierno alemán reafirmó estas decisiones de políticas públicas declarando, además, que pretendía ser el líder global en la adopción de estas tecnologías, sin perjuicio de que, de manera paralela, se reservó el derecho a responder apropiadamente cuando el cifrado limitara severamente la acción de las agencias penales y del sistema de inteligencia (Herpig & Heumann, 2019). Alemania ha optado por el camino de entregarle a sus agencias estatales las capacidades técnicas necesarias para enfrentar los inconvenientes en el uso del cifrado antes que promover el desarrollo de puertas traseras, que suelen volver inseguras este tipo de tecnologías. En el caso de Francia, luego de los atentados terroristas del año 2015, los legisladores franceses han estado a punto de aprobar un paquete legislativo que exigía a las empresas proveedores de servicios y productos encriptados que garantizaran el acceso de las autoridades de gobierno en el contexto de investigaciones

11 Las denominadas «puertas traseras» son mecanismos de acceso a contenidos o dispositivos que utilizan algún tipo de encriptación, mediante los cuales el fabricante del dispositivo o aplicación puede, sin notificar al dueño de este, burlar las medidas de seguridad utilizadas.

criminales y terroristas. Sin embargo, esta iniciativa fracasó por un solo voto en la Asamblea Nacional de Francia (Acharya, Bankston, Schulman & Wilson, 2017).

La lucha contra el terrorismo también ha sido el factor que ha motivado la discusión dentro de la Unión Europea sobre la regulación del uso de herramientas de cifrado de comunicaciones privadas. Los diversos ataques ocurridos durante los años 2014, 2016 y 2017 en ciudades como París, Londres o Bruselas —por mencionar a algunos— movilizaron, primero, una respuesta que apunta al fortalecimiento de las capacidades investigativas de Europol y de las policías nacionales de los Estados miembros de la Unión. Segundo, se dio inicio a procesos de consultas a diferentes partes interesadas con miras a eventuales procesos regulatorios. Desde la dimensión de la persecución criminal, el reporte «Internet Organised Crime Threat Assessment» señala que el uso de herramientas de anonimato y cifrado para fines ilegales «representa un grave impedimento para la detección, investigación y enjuiciamiento de delincuentes» (Europol, 28 de setiembre de 2016, p. 5). Con estos antecedentes, algunos países (The White House, Office of the Press Secretary, 16 de enero de 2015) han dado señales públicas de querer avanzar en el establecimiento de reglas nacionales, mientras que otro grupo de países (Stupp, 22 de noviembre de 2016) ha solicitado a la Unión Europea que se discutan y adopten reglas comunes para limitar la encriptación de mensajes o para facilitar el acceso de las organizaciones responsables de las investigaciones criminales a contenidos o dispositivos protegidos mediante encriptación, ya sea mediante la instalación de «puertas traseras» o la promoción de herramientas de cifrado débiles.

De momento, estas opciones parecen estar descartadas. Conforme señala la comunicación conjunta de la Comisión Europea y la Alta Representante de la Unión para Asuntos Exteriores y Políticas de Seguridad, la «encriptación fuerte es la base de los sistemas seguros de identificación digital que desempeñan un papel clave en la eficacia de la ciberseguridad; también protege la propiedad intelectual de las personas y garantiza derechos fundamentales, como la libertad de expresión y la protección de los datos personales, además de garantizar un comercio en línea seguro» (Comunicación Conjunta al Parlamento Europeo y al Consejo. Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE, p. 11). En similar sentido se ha pronunciado Comisión Europea, la cual —citando además el artículo 32 del Reglamento General de Protección de Datos Personales— sostiene que «[e]l uso del cifrado es esencial para asegurar la ciberseguridad y la protección de los datos personales. La legislación de la UE recoge específicamente la función del cifrado para garantizar un nivel apropiado de seguridad en el tratamiento de datos personales» (Comunicación de la Comisión al Parlamento

Europeo, al Consejo Europeo y al Consejo. 2017. Undécimo informe de evolución hacia una Unión de la Seguridad genuina y efectiva, p. 9).

De momento, tal como claramente identifica Maria Koomen, la posición de la Unión Europea transita desde la opción regulatoria aparentemente descartada a una estrategia de fortalecimiento de las capacidades técnicas de los organismos de investigación criminal, que incluye «un enfoque más práctico para desarrollar las técnicas y capacidades de los estados miembros para acceder a datos encriptados» (Koomen, 2019, p. 6). Con esto, formará parte del mandato de la Comisión Europea, durante lo que queda del año 2019 y los próximos cuatro años, mantener el diálogo público y privado sobre las implicancias técnicas, económicas, políticas y legales del uso de herramientas de cifrado y su regulación dentro de las fronteras de la Unión, con las complejidades propias de un asunto que entrecruza la protección de la seguridad de los Estados y sus habitantes y el amparo de diversos derechos fundamentales, como veremos a continuación.

IV. ASPECTOS JURÍDICOS DEL CIFRADO

En razón de los posibles usos duales de las herramientas de cifrado, esto es, para proteger información digital o ciertas comunicaciones sensibles o como herramienta para encubrir ilícitos, su utilización resulta interesante y relevante para el derecho. El cifrado de comunicaciones privadas puede ser analizado —desde una perspectiva jurídicamente relevante— desde dos ámbitos aparentemente opuestos o que pudieran comprenderse, en una primera mirada, como contradictorios. Por una parte, el cifrado eleva el estándar de protección de la privacidad y de la inviolabilidad de las comunicaciones privadas a través del uso de herramientas técnicas que tornan inaccesibles los contenidos de estas. Esto redunda en la mejor protección de todo tipo de comunicaciones y especialmente de aquellas que dan cuenta de algún tipo de contenidos o relaciones sensibles como en los casos donde existe alguna obligación legal de secreto. Sería el caso, por ejemplo, de las comunicaciones amparadas por el secreto profesional, la reserva de las fuentes en el ejercicio del periodismo, las comunicaciones en el ámbito de los sistemas de inteligencia y la seguridad nacional, entre otras.

En el Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión de Naciones Unidas, se sostiene al respecto lo siguiente:

> El cifrado y el anonimato, y los conceptos de seguridad subyacentes, proporcionan la privacidad y seguridad necesarias para el ejercicio del derecho a la libertad de opinión y de expresión en la era digital. Dicha seguridad puede ser esencial para el ejercicio de otros derechos,

> incluidos los derechos económicos, el derecho a la vida privada, a un juicio con las debidas garantías, a la libertad de reunión y de asociación pacíficas, y el derecho a la vida y a la integridad física. Debido a su importancia para los derechos de libertad de opinión y de expresión, las restricciones al cifrado y el anonimato deben limitarse de forma estricta, de conformidad con los principios de legalidad, necesidad, proporcionalidad y legitimidad del objetivo (Asamblea General de Naciones Unidas, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, David Kaye, p. 21).

Desde la otra perspectiva, el cifrado puede representar un riesgo para el ejercicio de las funciones jurisdiccionales y la protección efectiva de algunos derechos humanos como el derecho de acceso a la información pública o, incluso, para la seguridad pública o para la eficacia en el ejercicio de la acción punitiva del Estado. Así, por ejemplo, el uso del cifrado de comunicaciones podría significar la imposibilidad de acceder a determinados medios probatorios en un procedimiento judicial o restringir los mecanismos de control sobre las agencias del sistema de inteligencia, por mencionar algunos casos.

En el caso específico del procedimiento penal, espacio por antonomasia de ejercicio de la acción punitiva del Estado, existen una serie de derechos constitucionales enmarcados en el principio general del debido proceso que entran en directa relación —complementaria o contradictoria según sea el interviniente de que se trate— con el cifrado de comunicaciones. Así, por ejemplo, la garantía de no autoincriminación contenida en el literal f) del numeral 7 del artículo 19 de la Constitución chilena, podría servir de sustento a la afirmación de que un imputado tiene derecho al cifrado de sus comunicaciones privadas. Por su parte, la víctima en el proceso penal tendría expectativas razonables de que el Estado, en el ejercicio privativo de la acción punitiva y en aras de la eficacia del proceso, dispusiera de la totalidad de los medios probatorios disponibles, incluyendo aquellos que hayan sido objeto de encriptación.

Lawrence Lessig sostiene que las «tecnologías de encriptación constituyen el avance tecnológico más importante de los últimos dos mil años», pero son un arma de doble filo, pues —continúa Lessig citando a Baker y Hurst— se trata «seguramente, de la mejor tecnología existente y, al mismo tiempo, la peor de ellas. Es capaz de frenar la delincuencia y de crear nuevos delitos» (Lessig, 2001, p. 77). De esta manera, es posible identificar una tensión no resuelta entre las funciones que desempeña el cifrado de las comunicaciones privadas —en tanto medio técnico que profundiza el ejercicio de los derechos a la privacidad y a la inviolabilidad de las comunicaciones— y la seguridad pública (Tomás, 2014).

V. LA (NO)REGULACIÓN DEL CIFRADO EN CHILE

En Chile, el cifrado no está regulado[12]. Para el derecho chileno, el cifrado simplemente no existe. No hay jurisprudencia judicial ni administrativa que se refiera a estas herramientas y no existen estudios doctrinarios acerca de los efectos jurídicos de su utilización. A nivel de planificación política, la Política Nacional de Ciberseguridad del gobierno de Chile sostiene expresamente lo siguiente:

> esta política reconoce el valor de las tecnologías de cifrado, que permiten dotar de niveles de confidencialidad e integridad de la información sin precedentes en nuestra historia. Las medidas basadas en esta política deberán promover la adopción de cifrado punto a punto para los usuarios, en línea con los estándares internacionales; y en ningún caso se promoverá el uso intencional de tecnologías poco seguras, ni la obligación a ninguna persona u organización que provea servicios digitales, de implementar mecanismos de «puerta trasera» que comprometan o eleven los riesgos asociados a las tecnologías de seguridad empleadas (p. 13).

Por ello, resulta relevante identificar la tensión que produciría la utilización de herramientas de cifrado de comunicaciones privadas en el derecho chileno, en especial, la tensión que se produciría en el ejercicio del denominado bloque constitucional de protección de la vida privada y la eficacia de las medidas de seguridad pública. Para identificar adecuadamente esta tensión, primero deberemos describir, analizar y comprender el derecho a la vida privada y el derecho a la inviolabilidad de las comunicaciones en el derecho constitucional chileno, para luego caracterizar el concepto de seguridad pública y sus implicancias normativas.

V.1. La protección de la privacidad en el derecho constitucional chileno

En el derecho constitucional chileno existe un conjunto de derechos expresos —y también algunos derechos implícitos—[13] que ampara aquello que intuitivamente denominamos privacidad, de una forma mucho más amplia y comprensiva que como la doctrina tradicionalmente lo ha tratado y analizado en las últimas décadas. Esta amplitud resulta imprescindible si queremos utilizar el derecho a la privacidad como una de las defensas frente a las amenazas y riesgos que ha supuesto y supone el uso intensivo de tecnologías digitales en la vida cotidiana

12 De manera indirecta, la Ley 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de certificación de dicha firma regula, sin decirlo expresamente, algunos de los efectos del cifrado en la medida en que las firmas electrónicas requieren de algún tipo de tecnología de cifrado para ser seguras, confiables e integras.

13 En la doctrina usualmente se incorpora en esta categoría al derecho sobre la imagen propia, el cual no será analizado en el presente trabajo.

de las personas, especialmente los usos corporativos, comerciales y gubernamentales vinculados especialmente a la seguridad pública y la vigilancia masiva[14].

A partir del texto constitucional de 1980 —que reconoció la protección de la vida privada como derecho independiente— y las reformas constitucionales del año 2005 —que eliminó la referencia la protección de la vida pública de las personas (Ley 20.050, artículo 1, numeral 10, literal b)— y del año 2018 —que agregó expresamente la protección de datos personales (Ley 21.096, artículo único)—, en Chile contamos con un sistema de protección de la privacidad compuesto por cinco derechos perfectamente diferenciados entre sí. Se trata de (a) el derecho a la vida privada, (b) el derecho a la protección de datos personales, (c) el derecho a la inviolabilidad del hogar, (d) el derecho a la inviolabilidad de las comunicaciones privadas, y (e) el derecho a la inviolabilidad de los documentos privados. Estos cinco derechos, en conjunto con las normas pertinentes de los tratados internacionales sobre derechos humanos suscritos y ratificados por Chile y que se encuentren vigentes (véase Declaración Universal de Derechos Humanos, artículo 12; Pacto Internacional de Derechos Civiles y Políticos, artículo 17; Convención Americana sobre Derechos Humanos (Pacto de San José), artículo 11; Declaración Americana de Derechos y Deberes del Hombre, artículos V, IX y X), forman parte de lo que hemos denominado sistema constitucional de protección de la privacidad, que debiera servir a varios propósitos. Por una parte, servir de mandato constitucional para el legislador al momento de desarrollar, en el nivel legal, la protección efectiva de estos derechos; mandato para el juez al momento de interpretar y aplicar los derechos protegidos constitucionalmente; mandato para las autoridades públicas en el desempeño de sus funciones; entre otros (Álvarez, 2018).

Es de vital importancia diferenciar y caracterizar cada uno de los derechos que forman parte del sistema constitucional de protección de la privacidad en Chile, el cual está adquiriendo y adquirirá mayor relevancia y notoriedad por el avance del desarrollo de las tecnologías digitales de comunicación y la intensificación de su utilización en la sociedad chilena. No obstante lo anterior, para los propósitos de este trabajo únicamente describiremos el estado actual de la discusión del derecho a la vida privada y el derecho a la inviolabilidad de las comunicaciones privadas. Una de las principales dificultades que ha experimentado la doctrina y la jurisprudencia nacional para el desarrollo de una teoría sobre el derecho a la vida privada ha consistido precisamente en definir el alcance del concepto en estudio y la determinación de los bienes

14 Sobre este punto, recomiendo revisar una de las obras más completas en castellano sobre el concepto de derecho a la vida privada, escrita por el profesor y jurista Eduardo Novoa Monreal durante su exilio en Venezuela (Novoa Monreal, 1979; también véanse Vial, 2000; Anguita, 2007; Corral, 2000a, 2000b; y, más recientemente, Figueroa, 2014; Álvarez, 2018).

jurídicos amparados por este derecho (Undurraga, 2005; Corral, 2000a, 2000b). Responder la pregunta acerca de qué es la vida privada suele sacarnos a pasear por consideraciones de tipo social, cultural, históricas, antropológicas e, incluso, religiosas (Novoa Monreal, 1979).

La protección de la inviolabilidad de los papeles y de la correspondencia privada tiene una larga tradición en el derecho constitucional chileno. Ya en los primeros textos constitucionales del Chile independiente, se resguardaban —además del hogar y los papeles—la correspondencia epistolar[15]. En la Constitución de 1980 se mantuvo esta tradición en el numeral 5 del artículo 19 que protege la inviolabilidad de toda forma de comunicación privada. El concepto de «comunicaciones privadas» se refiere a todo «acto comunicativo que se proyecta de una persona hacia otra (que pueden ser una o varias personas) quien ha sido escogida por el emisor y donde no importa el contenido ni el medio por el cual se materialice la comunicación» (Álvarez, 2019, p. 45. De esta manera, las llamadas telefónicas analógicas o digitales, los correos electrónicos intercambiados y los mensajes enviados por vía WhatsApp, Signal o Telegram son solo algunas de las formas que puede adoptar el acto comunicativo objeto de protección constitucional. Esta protección se verá reforzada —desde un punto de vista técnico— si en dichos actos comunicativos se utilizan herramientas de cifrado, lo que tendrá consecuencias, como hemos dicho, en el ámbito de la seguridad pública.

V.2. El concepto de seguridad pública en el derecho constitucional chileno

Desde que el cifrado computacional se masificó, pasando de ser una herramienta de uso exclusivamente militar y de inteligencia a ser parte de las opciones disponibles para los ciudadanos que quisiesen aumentar la privacidad de sus comunicaciones, se levantaron opiniones críticas a la utilización estas tecnologías por suponer un límite al ejercicio de las funciones propias de las autoridades encargadas de velar por el cumplimiento de la ley y la seguridad (Etzioni, 2012, p. 122). Dorothy Denning y William Baugh plantean cinco amenazas específicas del uso de encriptación en este ámbito: (a) puede imposibilitar la obtención de pruebas necesarias; (b) puede frustrar la obtención de inteligencia vital en la investigación criminal; (c) puede frustrar que se eviten ataques terroristas; (d) puede dificultar el trabajo de las agencias de inteligencia; y (e) puede provocar incluso mayores vulneraciones a la privacidad (1997). De las cinco amenazas descritas, las tres primeras comparten la

15 El artículo 138 (147) de la Constitución de 1833 establecía lo siguiente: «La correspondencia epistolar es inviolable. No podrá abrirse, ni interceptarse, ni registrarse los papeles o efectos, sino en los casos expresamente señalados en la ley».

característica de tratarse de las amenazas que el uso de las herramientas de cifrado supondría para la seguridad pública.

El concepto de seguridad dista de ser pacífico. Es una idea antigua y disputada, con discusiones en diversos frentes y disciplinas que se remontan, en la época contemporánea, a los fines de la Guerra Fría y, ciertamente, no es posible abordarlas de manera integral en este trabajo. A título meramente enunciativo, es posible identificar al menos las siguientes dimensiones del concepto de seguridad: seguridad nacional, seguridad humana, seguridad multidimensional, seguridad ciudadana y seguridad pública. Revisaremos sintéticamente este último concepto.

La seguridad pública es comprendida como la «garantía que debe brindar el Estado para el libre ejercicio de los derechos de todos los ciudadanos» (Valencia, 2002, p. 9). Engloba la defensa de las instituciones y mantenimiento de la paz y tranquilidad civil de amenazas internas, lo que la diferencia sustancialmente del concepto de seguridad exterior. La doctrina constitucional nacional chilena poco ha ahondado en el concepto de seguridad pública, atendido que se trata de una expresión utilizada —en el capítulo XI del texto constitucional vigente— únicamente para referirse a las instituciones policiales responsables del orden y seguridad pública interior, en una forma que pareciera sinónima del concepto indeterminado de «orden público» (García & Contreras, 2014, p. 817). Si tal aseveración es correcta —cuestión sobre la cual indagaremos en futuras investigaciones— la seguridad pública operaría: (a) como causal de limitación de ciertos derechos fundamentales (véanse, por ejemplo, los numerales 6, 11, 15 y 21 del artículo 19 de la Constitución Política); (b) como regla para la determinación de competencias de autoridades públicas, como el Presidente de la República (véase el inciso segundo del artículo 24 de la Constitución) o las Fuerzas de Orden y Seguridad Pública Interior (véase el inciso segundo del artículo 101 de la Constitución); y (c) su grave afectación constituye un requisito ineludible para decretar el estado de emergencia (véase el artículo 42 de la Constitución).

Por otra parte, cabe señalar que la Constitución sí utiliza otras concepciones de seguridad asociadas —algunas de ellas— a la doctrina de la seguridad nacional, que inspiraron las normas y prácticas de la dictadura cívico-militar que gobernó Chile entre 1973 y 1990. Según Pablo Contreras, en la Constitución se utilizan «distintos términos que, en ocasiones, se superponen en cuanto al contenido que protege la seguridad de la nación […] [tales como] "seguridad nacional", "seguridad pública", "seguridad externa" y "seguridad pública interior"» (2012, p. 47). Con todo, no ha sido posible encontrar un concepto específico de seguridad pública en la doctrina nacional que permita identificar los elementos sustanciales y formales que aclare, además, su naturaleza

jurídica. Esto, por cuanto, desde la teoría constitucional la seguridad pública puede ser comprendida y analizada de diversas maneras: como un bien común o colectivo (Alexy, 1994, p. 186) constitucionalmente protegido, como un derecho fundamental implícito (Valencia, 2002, p. 9) o como un interés legítimo del Estado, que operaría como límite de los derechos fundamentales de las personas[16]. Según cuál sea el enfoque escogido, dependerá la forma en que se resuelve la tensión entre seguridad pública y los derechos a la vida privada y a la inviolabilidad de las comunicaciones privadas.

Como concepto operativo para los propósitos de este texto, podemos comprender que la seguridad pública cumple la función normativa de límite externo[17] a ciertos derechos fundamentales, en particular y en lo pertinente a esta investigación, al derecho a la vida privada (Ramírez, 2016) y al derecho a la inviolabilidad de las comunicaciones privadas (Álvarez, 2019). Siguiendo las ideas de Robert Alexy, ambos derechos constitucionales deben entenderse de la manera más amplia posible (Contreras & Salgado, 2017, p. 218), pero sus contornos son delimitados —o restringidos para utilizar el lenguaje de Alexy— por otros derechos fundamentales o bienes constitucionales implícitos o explícitos (Nogueira, 2005). Para Alexy «no existe una relación necesaria entre el concepto de derecho y el de restricción. La relación es creada solo a través de una necesidad externa al derecho, de compatibilizar los derechos de diferentes individuos como así también los derechos individuales y los bienes colectivos» (2001, p. 268).

VI. ¿CÓMO SE RESUELVE ESTA TENSIÓN?

Para resolver adecuadamente la tensión identificada entre la seguridad pública y el derecho a la vida privada y el derecho a la inviolabilidad de las comunicaciones privadas por la utilización de herramientas de cifrado —cuestión que no abordaremos a fondo en este artículo ya que forma parte de una investigación más extensa—, resulta necesario recurrir a los elementos interpretativos propios de los derechos fundamentales. Aquí, como cuestión preliminar, cabe descartar desde ya —siguiendo a Ernst-Wolfgang Böckenförde— los métodos interpretativos clásicos, esto es, aquellos que fueron elaborados para interpretar la ley, los que comparten algunas deficiencias que dificultan o desaconsejan su utilización respecto de textos constitucionales (1993, p. 36). El mismo autor destaca que las

16 Tal como sostiene Gregorio Peces-Barba, la discusión doctrinaria sobre los límites a los derechos fundamentales no ha tenido un desarrollo suficiente, ya sea porque se confunde con otros debates interesantes, como el relativo al contenido esencial del derecho o porque derechamente ha sido ignorado (1999, pp. 587 y ss.).

17 Sobre la discusión acerca de los límites internos y externos a los derechos fundamentales, véase Aguiar de Luque (1993) y Prieto (2000). En el derecho constitucional chileno destaca la obra de Aldunate (2008).

características propias de las disposiciones sobre derechos fundamentales —construidas como fórmulas lapidarias y preceptos de principios que carecen de un único sentido material— (p. 44), su textura abierta, fragmentariedad y vigencia como derecho directamente aplicable hacen de la interpretación constitucional una herramienta de especial importancia y trascendencia (p. 126). Por ello, deberemos explorar otras formas de solución de conflictos constitucionales para intentar resolver la tensión o los conflictos que se pueden generar en la relación entre la seguridad pública —ya sea que la entendamos como bien común o colectivo constitucionalmente protegido, como un derecho fundamental implícito o como un interés legítimo del Estado— y los derechos a la vida privada, y a la inviolabilidad de las comunicaciones privadas. Para ello, debo prevenir, es fundamental determinar previamente la naturaleza jurídica del concepto de seguridad pública y, de ahí, examinar si, por ejemplo, la aplicación del principio de proporcionalidad utilizada en el contexto de la teoría de los límites externos resulta idónea para resolver la tensión que preliminarmente hemos identificado, todas cuestiones que serán analizadas en obras posteriores[18].

Tal como hemos sostenido previamente, identificar «formas idóneas, legítimas y democráticas para resolver la tensión entre privacidad y seguridad puede ayudar a racionalizar o incluso proscribir la utilización de medidas que pueden ser restrictivas en el ejercicio de ciertos derechos fundamentales, especialmente aquellas que implican un uso intensivo de tecnologías para la vigilancia» (Álvarez & Bravo, 2018; Bauman & Lyon, 2013) y el control de los ciudadanos (Tejerina, 2014) en una sociedad altamente tecnologizada y conectada como la chilena. Como bien apunta Jacqueline de Souza Abreu, la pregunta sobre una eventual regulación de las tecnologías de cifrado pasa necesariamente por contar con evidencia suficiente respecto a los efectos reales del cifrado como restricción de las capacidades de investigación penal del Estado, además de realizar una evaluación de riesgos que supone cualquier regulación del cifrado para la ciberseguridad, ya sea individual, colectiva o nacional y para los derechos humanos (Souza Abreu, 2017).

VII. CONCLUSIONES

En este trabajo hemos explorado, sintéticamente, la evolución que han experimentado las herramientas de cifrado de comunicaciones en las últimas décadas, en especial a partir del término de la II Guerra Mundial y del desarrollo de las tecnologías computacionales y digitales, constatando el importante rol que hoy desempeñan para garantizar

18 Para una buena síntesis del debate nacional y comparado sobre la utilización del principio de proporcionalidad en materia de derechos fundamentales, véase Contesse (2017, pp. 285 y ss.) y Bordalí (2003, pp. 64 y ss.).

la seguridad y privacidad de las comunicaciones, en especial, desde el surgimiento de las tecnologías de encriptación *end to end*. Vimos cómo el uso de herramientas de cifrado de comunicaciones transitó desde ser un asunto exclusivamente radicado en el sistema de inteligencia norteamericano hacia el espacio del debate constitucional, en especial respecto a la protección constitucional que este tipo de tecnologías podría encontrar en derechos clásicos como el derecho a la libertad de expresión, en tanto discurso protegido, o el derecho a la privacidad implícito en la Cuarta Enmienda de la Constitución de Estados Unidos. Pudimos constatar que este debate continuará abierto. En el caso de Europa, pudimos revisar cómo el debate ha tenido lugar únicamente a nivel pre-regulatorio en diversas agencias supranacionales de la Unión Europea, sin perjuicio de algunos debates que han tenido lugar en algunas legislaciones nacionales. Con todo, pudimos apreciar que se trata de discusiones abiertas que no han generado consensos mínimos para ser formalizados en algún tipo de instrumento jurídico vinculante.

Finalmente, en el caso del derecho chileno, hemos identificado los dos principales bienes jurídicos en juego que deben ser tomados en consideración al momento de resolver la tensión que se produce por el uso de herramientas de cifrado de comunicaciones respecto del ejercicio del derecho fundamental a la privacidad y el bien jurídico constitucional denominado seguridad pública, entendida como límite al ejercicio de esos derechos fundamentales. Como dijimos, las formas de resolver esta tensión serán abordadas en trabajos posteriores, toda vez que el desarrollo doctrinario chileno en estas materias resulta todavía insuficiente.

REFERENCIAS

Abel, R. (24 de octubre de 2017). FBI Director Wray: Encryption Kept Agency from Accessing 7,000 Mobile Devices. *SC Media*. Recuperado de https://www.scmagazine.com/fbi-director-argues-encryption-inhibiting-cases/article/702462/

Acharya, B., Bankston, K., Schulman, R., & Wilson, A. (2017). *Deciphering the European Encryption Debate: France*. Policy Paper. Washington D.C.: New America-Open Technology Institute. Recuperado de https://www.newamerica.org/oti/policy-papers/deciphering-european-encryption-debate-france/

Aguiar de Luque, L. (1993). Los límites de los derechos fundamentales. *Revista Centro de Estudios Constitucionales*, *14*(enero-abril), 9-34.

Aldunate, E. (2008). *Derechos fundamentales*. Santiago de Chile: Thomson Reuters.

Alexy, R. (1994). *El concepto y la validez del derecho y otros ensayos*. Barcelona: Gedisa.

Alexy, R. (2001). *Teoría de los derechos fundamentales*. Madrid: Centro de Estudios Políticos y Constitucionales.

Álvarez, D. (2018). Privacidad en línea en la jurisprudencia constitucional chilena. *Revista de Derecho Público*, 89, 11-32. doi: https://doi.org/10.5354/0719-5249.2018.52027

Álvarez, D. (2019). *La inviolabilidad de las comunicaciones privadas electrónicas*. Santiago de Chile: LOM Ediciones.

Álvarez, D. & Bravo, C. (2018). Caso Huracán: ¿es factible técnica y legalmente «hackear» WhatsApp? *CIPER Chile*. Recuperado de https://ciperchile.cl/2018/02/07/caso-huracan-es-factible-tecnica-y-legalmente-hackear-whatsapp/

Anguita, P. (2007). *La protección de datos personales y el derecho a la vida privada*. Santiago de Chile. Editorial Jurídica.

Assange, J. (2013). *Criptopunks: la libertad y el futuro de Internet* (Trad. Nicolás Lerner). Santiago de Chile. LOM Ediciones.

Bauman, Z. & Lyon, D. (2013). *Vigilancia líquida* (Trad. Alicia Capel). Barcelona: Paidós.

Böckenförde, E.-W. (1993). *Escritos sobre derechos fundamentales*. Baden-Baden: Nomos.

Bordalí, A. (2003). *Temas de derecho procesal constitucional*. Santiago de Chile: Fallos del Mes.

Calo, R. (2016). Can Americans Resist Surveillance? *The University of Chicago Law Review*, *83*(1), 23-43. Recuperado de https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=5917&context=uclrev

Castells, M. (s.f.). *Internet y la sociedad red*. Conferencia inaugural del programa de doctorado sobre Sociedad de la Información y el Conocimiento, Universitat Oberta de Catalunya. Recuperado de http://red.pucp.edu.pe/wp-content/uploads/biblioteca/Castells_internet.pdf

Castells, M. (1999). *La era de la información: economía, sociedad y cultura*. Ciudad de México: Siglo XXI.

Cohn, C. (2014). Nine Epic Failures of Regulating Cryptography. *Electronic Frontier Foundation*, 26 de setiembre. Recuperado de https://www.eff.org/deeplinks/2014/09/nine-epic-failures-regulating-cryptography

Contesse, J. (2017). Proporcionalidad y derechos fundamentales. En P. Contreras y C. Salgado (Eds.), *Manual de derechos fundamentales* (pp. 285-322). Santiago de Chile: LOM Ediciones.

Contreras, P. (2012). *Secretos de Estado: transparencia y seguridad nacional*. Santiago de Chile: Thomson Reuters.

Contreras, P. & Salgado, C. (2017). *Manual de derechos fundamentales*. Santiago: LOM Ediciones.

Corral, H. (2000a). Configuración jurídica del derecho a la privacidad I: origen, desarrollo y fundamentos. *Revista de Derecho - Pontificia Universidad Católica de Valparaíso*, *27*(1), 51-79.

Corral, H. (2000b). Configuración jurídica del derecho a la privacidad II: concepto y delimitación. *Revista de Derecho - Pontificia Universidad Católica de Valparaíso*, *27*(2), 331-355.

Denning, D.E. & Baugh, W.E. (1997). Encryption and Evolving Technologies: Tools of Organized Crime and Terrorism. *Trends in Organized Crime*, *3*(1), 84-91. doi: https://doi.org/10.1007/s12117-997-1149-1

Etzioni, A. (2012). *Los límites de la privacidad* (Trad. Alexander López). Buenos Aires: B de F.

Etzioni, A. (2015). Ultimate Encryption. *South Carolina Law Review*, *67*(3), 561-583. doi: https://doi.org/10.2139/ssrn.2605153

European Police Office (Europol). (28 de setiembre de 2016). *The Internet Organised Crime Threat Assessment (IOCTA) 2016*. Recuperado de https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

Figueroa, R. (2014). *Privacidad*. Santiago de Chile: Ediciones Universidad Diego Portales.

Galende, J. (2000). Sistemas criptográficos empleados en Hispanoamérica. *Revista Complutense de Historia de América*, *26*, 57-71.

García, G. & Contreras, P. (2014). *Diccionario constitucional chileno*. Santiago de Chile: Cuadernos del Tribunal Constitucional.

Granados, G. (2006). Introducción a la criptografía. *Revista Digital Universitaria*, *7*(7), s.p. Recuperado de http://www.revista.unam.mx/vol.7/num7/art55/int55.htm

Gonzalez, O. (2019). Cracks in the Armor: Legal Approaches to Encryption. *University of Illinois Journal of Law, Technology & Policy*, *1*, 1-48. doi: https://doi.org/10.2139/ssrn.3035045

Herpig, S. & Heumann, S. (2019). The Encryption Debate in Germany. *Carnegie Endowment for International Peace*. Recuperado de https://carnegieendowment.org/2019/05/30/encryption-debate-in-germany-pub-79215

Israeli Firm Helping FBI to Open Encrypted iPhone: Report. (23 de marzo de 2016). *Reuters*. Recuperado de http://www.reuters.com/article/us-apple-encryption-cellebrite-idUSKCN0WP17J

Kerr, O. & Schneier, B. (2018). Encryption Workarounds. *Georgetown Law Journal*, *106*, 989-1019. doi: http://dx.doi.org/10.2139/ssrn.2938033

Koomen, M. (2019). The Encryption Debate in the European Union. *Carnegie Endowment for International Peace*. Recuperado de https://carnegieendowment.org/2019/05/30/encryption-debate-in-european-union-pub-79220

Lessig, L. (2001). *El código y otras leyes del ciberespacio* (Trad. Ernesto Alberola). Madrid: Taurus.

Levy, S. (2002). *Cripto. Cómo los informáticos libertarios vencieron al gobierno y salvaguardaron la intimidad en la era digital*. Madrid: Alianza.

Mattelart, A. & Vitalis, A. (2015). *De Orwell al cibercontrol*. Barcelona: Gedisa.

McClure, D. (2000). First Amendment Freedoms and the Encryption Export Battle: Deciphering the Importance of *Berstein v. United States Department of Justice*, 176 F.3d 1132 (9th Cir. 1999). *Nebraska Law Review*, *79*(2), 465-284.

Nogueira, H. (2005). Aspectos de una teoría de los derechos fundamentales: la delimitación, regulación, garantías y limitaciones de los derechos fundamentales. *Ius et Praxis*, *11*(2), 15-64. doi: https://doi.org/10.4067/s0718-00122005000200002

Novoa Monreal, E. (1979). *Derecho a la vida privada y libertad de información: un conflicto de derechos*. Ciudad de México: Siglo XXI.

Peces-Barba, G. (1999). *Curso de derechos fundamentales: teoría general*. Madrid: Universidad Carlos IIR-Boletín Oficial del Estado.

Post, R. (2000). Encryption Source Code and the First Amendment. *Berkeley Technology Law Journal*, *15*(2), 713-723. doi: https://doi.org/10.2139/ssrn.238191

Prieto, L. (2000). La limitación de los derechos fundamentales y la norma de clausura del sistema de libertades. *Pensamiento Constitucional*, *8*(8), 61-102.

Ramírez, T. (2016). Nuevas tecnologías al servicio de la seguridad pública y afectación de la privacidad: criterios de ponderación. *Revista Chilena de Derecho y Tecnología*, *5*(1), 57-86. doi: https://doi.org/10.5354/0719-2584.2016.41688

Sainz, J. (1991). Estudio de «inteligencia operacional». *Cuadernos de estrategia*, *31*, 15-37.

Singh, S. (2000). *Los códigos secretos*. Madrid: Debate.

Souza Abreu, J. de (2017). Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. *Revista Brasileira de Políticas Públicas, 7*(3), 25-42. doi: https://doi.org/10.5102/rbpp.v7i3.4869

Stupp, C. (22 de noviembre de 2016). Five Member States Want EU-wide Laws on Encryption. *Euractiv*. Recuperado de https://www.euractiv.com/section/social-europe-jobs/news/five-member-states-want-eu-wide-laws-on-encryption

Swire, P. (2012). From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud. *International Data Privacy Law*, *2*(4), 200-206. doi: https://doi.org/10.1093/idpl/ips025

Tejerina, O. (2014). *Seguridad del Estado y privacidad*. Madrid: Reus.

The White House, Office of the Press Secretary. (16 de enero de 2015). *Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference*. Recuperado de https://www.whitehouse.gov/the-press-office/2015/01/16/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint-

Thiber. (11 de noviembre de 2013). *La Agencia de Seguridad Nacional (NSA), el espionaje y colaboración público-privada en EEUU*. Recuperado de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari41-2013-thiber-nsa-espionaje-colaboracion-publico-privada-snowden

Tomás, B. (2014). Privacidad versus seguridad en el ámbito europeo. En A. Fayos Gardó (Coord.), *Los derechos a la intimidad y a la privacidad en el siglo XXI* (pp. 215-241). Barcelona: Dykinson.

Undurraga, V. (2005). La privacidad como bien jurídico. En J.C. Varas y S. Turner (Coords.), *Estudios de derecho civil: jornadas nacionales de derecho civil* (pp. 509-530). Santiago de Chile: LexisNexis.

Valencia, V. (2002). *La seguridad pública como un derecho humano*. Ciudad de México: Comisión de Derechos Humanos del Estado de México.

Velasco, J. (20 de mayo de 2014). Breve historia de la criptografía. *DiarioTuring*. Recuperado de https://www.eldiario.es/turing/criptografia/Breve-historia-criptografia_0_261773822.html

Vial, T. (2000). Hacia la construcción de un concepto constitucional del derecho a la vida privada. *Revista Persona y Sociedad*, *XIV*(3), 47-68.

Jurisprudencia, normativa y otros documentos legales

Asamblea General de Naciones Unidas. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, David Kaye. Consejo de Derechos Humanos, 29 periodo de sesiones, 22 de mayo de 2015. A/HRC/29/32.

Bernstein v. United States Department of State. 176 F.3d 1132, Court of Appeals for the 9th Circuit.

Comisión Europea. Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo. 2017. Undécimo informe de evolución hacia una Unión de la Seguridad genuina y efectiva. Bruselas, 18 de octubre de 2017. COM(2017) 608 final. Recuperado de http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0608&from=ES

Comisión Europea, Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Comunicación Conjunta al Parlamento Europeo y al Consejo. Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE. Bruselas, 13 de setiembre de 2017. JOIN(2017) 450 final. Recuperado de https://ec.europa.eu/transparency/regdoc/rep/10101/2017/ES/JOIN-2017-450-F1-ES-MAIN-PART-1.PDF

Convención Americana sobre Derechos Humanos (Pacto de San José). Suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos (B-32). San José, Costa Rica, 7-22 de noviembre de 1969. Recuperado de https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm

Declaración Americana de Derechos y Deberes del Hombre. Aprobada en la Novena Conferencia Internacional Americana. Bogotá, Colombia, 1948. Recuperado de http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp

Declaración Universal de Derechos Humanos. Proclamada por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948 en su Resolución 217 A (III). Recuperado de https://www.un.org/es/universal-declaration-human-rights/

Export Administration Regulations [EAR]. Recuperado de https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

Foreign Intelligence Surveillance Act of 1978 [FISA]. 50 U.S. Code ch. 36. Recuperado de https://www.law.cornell.edu/uscode/text/50/chapter-36

Ley 20.050 [Chile]. Reforma constitucional que introduce diversas modificaciones a la Constitución Política del Estado. *Diario Oficial*, 25 de agosto de 2005.

Ley 21.096 [Chile]. Ley que consagra el derecho a protección de los datos personales. *Diario Oficial*, 16 de junio de 2018.

Memorandum for the Secretary of State and the Secretary of Defense. SUBJECT: Communications Intelligence Activities. Memorándum del Presidente Harry S. Truman, del 24 de octubre de 1952. Recuperado de https://www.nsa.gov/news-features/declassified-documents/nsa-60th-timeline/assets/files/1950s/19521024_1950_Doc_3978766_Comms.pdf

Pacto Internacional de Derechos Civiles y Políticos. Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966. Recuperado de https://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

Política Nacional de Ciberseguridad. 2017-2022. Gobierno de Chile. Recuperado de https://www.ciberseguridad.gob.cl/media/2018/06/PNCS_Chile_ES_FEA.pdf

USA PATRIOT Act: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. (2001). H.R.3162. Recuperado de https://www.congress.gov/bill/107th-congress/house-bill/3162

Wire and Electronic Communications Interception and Interception of Oral Communications. 18 U.S. Code ch. 119. Recuperado de https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119

Recibido: 03/06/2019
Aprobado: 14/10/2019