DERECHOS DIGITALES
América Latina

TECNOLOGÍAS PARA LA PRIVACIDAD Y LA LIBERTAD DE EXPRESIÓN: REGLAS SOBRE ANONIMATO Y CIFRADO

CHILE EN EL CONTEXTO LATINOAMERICANO

VALENTINA HERNÁNDEZ BAUZÁ

TECNOLOGÍAS PARA LA PRIVACIDAD Y LA LIBERTAD DE EXPRESIÓN: REGLAS SOBRE ANONIMATO Y CIFRADO

CHILE EN EL CONTEXTO LATINOAMERICANO

VALENTINA HERNÁNDEZ BAUZÁ

Portada y diagramación:Violeta Cereceda
Edición y correcciones: Vladimir Garay.
Diciembre de 2017.

Este informe fue realizado por Derechos Digitales, con el financiamiento
de Privacy International.

Derechos Digitales es una organización independiente y sin fines de lucro, fundada en el año 2005 y cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en el entorno digital, desde el interés público. Entre sus principales ejes de interés está la defensa y promoción la libertad de expresión, el acceso a la cultura y la privacidad.

1. RESUMEN EJECUTIVO[1]

Anonimato y cifrado son conceptos distintos, pero relacionados en el entorno digital. El anonimato consiste en ocultar la identidad del sujeto emisor de un mensaje (tanto en el nombre como en sus demás dimensiones), sin necesariamente ocultar el contenido de lo emitido. El cifrado del mensaje oculta su contenido, pero no necesariamente los datos de la comunicación misma que hacen identificable a quienes realizan el acto comunicativo. Para asegurar el derecho a la privacidad en la época de las tecnologías digitales, ambas técnicas deben actuar en conjunto.

El cuestionamiento al anonimato y al cifrado ha sido una parte fundamental de la agenda global contra la delincuencia organizada y el terrorismo, argumentándose que estas técnicas son utilizadas por criminales altamente capacitados en habilidades informáticas para coordinar su actuar.

La discusión entre los partidarios de comunicaciones anónimas e indescifrables y quienes buscan establecer medidas tecnológicas que permitan romper el cerrojo del cifrado no es nueva, pero el debate acompaña al aumento en el uso de estas medidas. El escenario actual es uno de posiciones ubicadas en extremos opuestos: por un lado, las agencias estatales de investigación y persecución criminal y por el otro, las empresas de tecnología que se resisten a introducir vulnerabilidades a sus equipos para evitar comprometer la seguridad del tráfico en línea, además de dar tranquilidad a sus usuarios. Pero en ambos casos, se trata de estados desarrollados o empresas poderosas, con un importante control sobre los flujos mundiales tanto financieros como de información.

Organismos como el Consejo de Derechos Humanos de las Naciones Unidas o la Comisión Interamericana de Derechos Humanos, a través de sus Relatorías Especiales para la Libertad de Expresión, han recalcado que el uso de herramientas de anonimato y cifrado son claves para tutelar adecuadamente el derecho a la privacidad y con ello garantizar otros derechos como la libertad de expresión.

Dentro de las medidas propuestas por los sectores que ven una amenaza en el uso de tecnologías de cifrado se encuentra introducir vulnerabilidades a los sistemas, solicitar copias de las llaves que permiten descifrar el contenido oculto y entregar capacidades técnicas y autorizaciones para romper el cifrado, a través de la fuerza bruta. Todas aquellas presentan riesgos diferentes, no solo a los derechos y libertades fundamentales de los usuarios, sino que al tráfico seguro de la red, el que se vería expuesto no solo al ingreso de los funcionarios públicos autorizados para aquello, sino también a hackers y otros individuos con intenciones maliciosas.

Existen al menos tres intereses a considerar en la regulación de estas materias: la seguridad pública, el derecho a la privacidad y la seguridad en los intercambios de información en línea. Por lo mismo, las soluciones deben equilibrarles en conjunto.

Se propone que se permita el acceso a contenidos o fragmentos de comunicación en específico previa orden judicial, resguardando así todos los intereses en juego, como también que se capacite a los funcionarios encargados de la labor de investigación, prevención y persecución delictiva para que estén en mejores condiciones de afrontar la actividad criminal digital, pudiendo prever y combatir esta última de forma más efectiva, eludiendo las acciones más gravosas respecto de la privacidad y otros derechos, recurriendo a las medidas de acceso como último recurso. Muy especialmente, se rechaza la noción de la introducción de vulnerabilidades, así como también la acción de hackeo por parte del estado destinada a la obtención de información tanto sobre la identidad de las personas como sobre el contenido de sus comunicaciones.

---

1 La autora agradece la estrecha colaboración del equipo técnico de Derechos Digitales.

Chile se encuentra en un contexto latinoamericano donde, afín a la tendencia regional, se muestran una tendencia a disminuir los ámbitos de anonimato digital, aun cuando, por regla general, no se encuentra prohibido. Si bien en el proceso de la Política Nacional de Ciberseguridad de Chile se reconoce el valor de la criptografía, las acciones gubernamentales tendientes a disminuir la capacidad de sostener comunicaciones de forma anónima han mantenido fuerza.

2. INTRODUCCIÓN: ANONIMATO Y CIFRADO

No es novedad que internet se ha posicionado como una forma de comunicación sumamente importante para informarse, comunicarse y expresar el parecer personal. La misma realidad es propia de Latinoamérica. Ya en el año 2010 se dijo que es la fuente más grande de información en el mundo.2 En efecto, la red es la principal fuente de telecomunicaciones, lo que solo se ha incrementado desde la masificación del uso de smartphones. Las amenazas que se derivan de aquello incluyen la actual capacidad técnica con que cuentan los gobiernos y los entes privados para vigilar a la población, interceptar comunicaciones y recolectar información sobre las personas.[3]

Esta capacidad de vigilancia implican un riesgo altamente acentuado sobre derechos fundamentales: quien sabe mi nombre, qué hago, dónde estoy, con quién hablo y qué digo, posee sobre mí capacidad de control. El uso de herramientas que permitan el anonimato en línea y el cifrado de las comunicaciones se han identificado como técnicas efectivas para recuperar algo de control sobre mi información, minimizar los riesgos de la vida en conexión y garantizar el respeto y ejercicio de derechos como la libertad de expresión y la privacidad.

Es por esta razón que la sociedad civil ha venido insistiendo en la importancia del respeto del anonimato y del uso de cifrado en línea como formas de protección ante vulneraciones y de ejercicio efectivo del derecho a la libertad de expresión.

El presente informe intenta dar ciertas luces sobre las reglas que rigen sobre el anonimato y el cifrado, con énfasis en Chile y en contraste con el contexto general de América Latina, desde una perspectiva normativa. Indicaremos cómo se pueden entender los conceptos de anonimato y cifrado a la luz de la sociedad actual y la tecnología disponible, para posteriormente tratar las regulaciones latinoamericanas sobre anonimato y cifrado, acabando con el detalle de la normativa chilena, determinando si las disposiciones, tanto regionales como nacional, permiten el uso de anonimato y cifrado, o si lo prohíben o entorpecen.

Principalmente, nuestros esfuerzos se concentran en el tratamiento del cifrado, tanto desde un punto de vista técnico como legal, resaltando su importancia para el resguardo y ejercicio de derechos fundamentales. Nos referimos a cómo se ha limitado normativamente la capacidad de mantener la reserva de identidad en línea y cómo se ha tratado de regular o limitar el cifrado, desatendiendo las características de internet y enfocándose solo en sus usos asociados a la actividad criminal, sin ponderar adecuadamente tanto las potenciales vulneraciones que ello puede causar en los derechos fundamentales enunciados como también en el tráfico seguro de la red.

---

2 DECCAN HERALD. 2010. Internet Now Single Biggest Source of Global Information. Deccan Herald. En línea, disponible en: http://www.deccanherald.com/content/117379/internet-now-single-biggest-source.html [fecha de consulta: 09 de febrero de 2016]

3 UNITED NATIONS. 2014. The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights. En línea, disponible en: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf [fecha de consulta: 09 de febrero de 2016] p. 3.

3. EL CRECIMIENTO DE INTERNET MÓVIL

Un estudio realizado el año 2014 por GSMA estima que, para el año 2020, América Latina será la segunda región con mayor cantidad de conexiones móviles a internet del mundo, en virtud del incremento de usuarios de teléfonos inteligentes, además del mejoramiento y migración a servicios de internet móvil de mayor velocidad como 3G, 4G,[4] y los estándares que les sucedan.

Chile igualmente ha presentado señas de la migración a internet, además de la tendencia a preferir los servicios de internet móvil. Un informe estadístico elaborado por la Subsecretaría de Telecomunicaciones (Subtel) en marzo de 2016 en relación al estado de las telecomunicaciones en el país en el año 2015, da cuenta de lo anterior, señalando que el 79.2 % de los accesos a internet en Chile se realizaron mediante servicios móviles, además de indicar un crecimiento de 14.1 % en dicho año de las suscripciones a servicios de telecomunicaciones de internet móvil, en contraste a la caída en cifras de uso de minutos en móviles, indicando esta Subsecretaría que en 2015 el tráfico total de voz fija y móvil bajó en un 2 %, hecho principalmente atribuible al uso de comunicaciones vía datos.[5]

Con tal base de usuarios compartiendo ideas, internet representa un entorno esencial para el ejercicio de derechos fundamentales. Dicho ejercicio de derechos es tutelado por los diversos sistemas legales al mismo nivel que los derechos fuera de la red: los mismos derechos que asisten a una persona offline, son plenamente aplicables online.[6]

---

4 GSMA. 2014. The Mobile Economy Latin America 2014. En línea, disponible en: http://www.gsmamobileeconomylatinamerica.com/GSMA_Mobile_Economy_LatinAmerica_2014.pdf [fecha de consulta: 09 de febrero de 2016] pp. 1-19.

5 CHILE. 2016. SUBTEL. Sector de Telecomunicaciones Cierre 2015. En línea, disponible en: http://www.subtel.gob.cl/wp-content/uploads/2015/04/PPT_Series_DICIEMBRE_2015_V5.pdf [fecha de consulta: 19 de abril de 2016] pp. 2-3.

6 UNITED NATIONS. 2012. General Assembly, Human Rights Council. Twentieth Session. Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development. En línea, disponible en: ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc [fecha de consulta: 25 de abril de 2015] p. 2.

4. ANONIMATO[7]

Entendemos por anonimato s una forma de comunicarse en la cual las personas no conocen el nombre de la persona que da origen al acto expresivo, escondiendo a la autora dicha información (Meo, 2010).

El concepto de anonimato no es reciente. La palabra tiene su origen en la voz griega anonymia, que significa "sin nombre".[8] Como señalan Solove, Rotenberg y Schwartz (2006) la idea misma de cubrirse para comunicarse es inherente al ser humano: el concepto de "persona" significa "máscara". Para los autores, esta máscara es una manifestación hecha con el fin de presentarnos frente al resto de la sociedad.

A través de la historia, la reserva o el secreto sobre la identidad de una persona (o un grupo de personas) ha sido fundamental para el ejercicio de derechos y libertades, especialmente de los derechos a la privacidad y libertad de expresión. Un ejemplo de esto es el caso McIntyre v Ohio Elections Commissions de la Corte Suprema de Justicia de los Estados Unidos de América, de 1995. Este fallo definió al anonimato como un escudo protector de la tiranía de la mayoría, siendo este reconocido y considerado como parte del contenido esencial de la Primera Enmienda a la Constitución estadounidense (que se entiende como consagratoria de la libertad de expresión), sirviendo como resguardo de las represalias que pueden tomar quienes no estén de acuerdo con la forma de pensar de quien se expresa (Grabow, 1997).

Considerando los avances tecnológicos, las capacidades de procesamiento de datos y la naturaleza de la red, no basta con ocultar el nombre para ser anónimo. Por ello, Gary T. Marx (2001) definió los elementos que componen la identidad de un individuo, entendiéndose a contrario sensu, que estos son los que deben ocultarse para asegurar un anonimato real. Ellos son:

- El nombre de la persona, tanto completo como parcial. Esto responde a la pregunta "quién".
- Datos de identificación tales que permitan localizar y encontrar al sujeto. Esto responde a la pregunta del "dónde". Acá podemos enmarcar, por ejemplo, el número de teléfono o la dirección de correo electrónico.
- Símbolos o secuencias de caracteres que puedan ser ligados a una persona –quién– o a un lugar o una dirección –dónde–. Por ejemplo, números de tarjetas bancarias, datos biométricos o la fecha de nacimiento, asociadas a personas específicas.
- Apodos, seudónimos o símbolos cuya vinculación a una persona determinada, a primera vista, no puede ser rastreada. Ello puede ser porque la misma ley o políticas de uso del servicio otorgan un número para acceder a este o recibir un resultado sin que en en momento alguno se proporcione el nombre del individuo (por ejemplo, un número generado por un servicio de salud para acceder a los resultados de un examen de VIH) o también aquellos casos en que el sujeto esté usando una identidad falsa en línea.
- Patrones de comportamiento o rasgos identificatorios referidos a la apariencia física de la persona. En gran medida a consecuencia del uso de herramientas tecnológicas, estos datos están ampliamente disponibles. Acá es donde quizás más resalta que aunque se desconozca el nombre de alguien, ello no implica que sea totalmente desconocido.

---

7 Este apartado toma como base lo discutido en Hernández (2016).

8 VOCABULARY.COM., "Anonymity". Vocabulary.com. En línea, disponible en: http://www.vocabulary.com/dictionary/anonymity [fecha de consulta: 05 de mayo de 2016]

- Las categorías sociales en las cuales puede ser clasificado un sujeto. Sexo, estrato socioeconómico, estado de salud, afiliaciones de cualquier tipo, entre otros ejemplos. El solo hecho de ser amigo de alguien o de encontrarse con un determinado grupo de personas en un lugar y momento puede ser clave para descifrar la identidad del individuo, o para atribuirle características que no posee o enmarcarlo en algún grupo, sin que realmente sea miembro.

- Finalmente, aquellas certificaciones que acrediten poseer un conocimiento o una preferencia en particular, los cuales pueden ir desde saber una contraseña, alguna señal visible que otorgue información de una persona (un uniforme o un tatuaje, por ejemplo), la posesión o compra de un objeto (un ticket para un recital) o poseer alguna habilidad ya sea física o intelectual (como lo sería hablar un idioma extranjero o saber conducir).

Si bien existe un reconocimiento histórico a la reserva de identidad en el discurso público, las herramientas tecnológicas limitan esa no identificación. Pero en este contexto de cantidades enormes de datos para identificar, el anonimato ha sido reconocido también como necesario a nivel del sistema interamericano de derechos humanos. Así ha sido especialmente desde la publicación de la Relatoría Especial Para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos del año 2013, titulada "Internet y Libertad de Expresión". En dicho informe, la Relatoría destaca la estrecha relación que existe entre los derechos a la privacidad y libertad de expresión, indicando que los Estados deben evitar implementar medidas que restrinjan de manera arbitraria o abusiva tales derechos.[9]

La Relatoría identifica como políticas concretas para proteger la privacidad y la libertad de expresión en línea al anonimato y a la protección de datos personales. Sobre anonimato, señala expresamente que la participación política sin revelar la identidad del emisor es una práctica usual en las democracias modernas y que, justamente, favorece a la expresión de ideas, en tanto protege al sujeto de represalias solo por su forma de pensar.[10]

No obstante, la misma Comisión Interamericana reconoce que el anonimato no ampara a todo tipo de discurso, así, no dispensa la protección del discurso anónimo a aquellos mensajes que excedan al contenido del derecho a la libertad de expresión (apología al odio o actividad criminal).[11]

La Corte Interamericana de Derechos Humanos en el fallo Escher v. Brasil (2009) si bien no se refiere específicamente a anonimato, reconoce protección no solo al contenido de una comunicación privada, sino también a "cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones".[12] Esto último es armónico con los postulados de Gary Marx sobre los elementos que actualmente componen la identidad de una persona, más allá de su nombre. Los metadatos, al ser analizados junto a otros datos, pueden dar suficientes señas del sujeto que navega a través de la red. Por ello, las técnicas de cifrado, en conjunción con el anonimato, son necesarias para resguardar a un cúmulo de derechos fundamentales que están sujetos a las amenazas que han nacido de la mano del desarrollo tecnológico.

---

9 COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, Relatoría Especial Para la Libertad de Expresión. "Libertad de Expresión e Internet". 2013, p. 63.

10 Ibíd., pp. 63-64.

11 Ibíd., p. 65.

12 CORTE INTERAMERICANA DE DERECHOS HUMANOS, Caso Escher y Otros v Brasil (Sentencia de 06 de julio de 2009). En línea, disponible en http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf [fecha de consulta: 19 de octubre de 2015] párrafo 114, p.34.

5. CIFRADO DE COMUNICACIONES

En el uso de la lengua castellana se ha discutido si el término correcto es cifrado o encriptación, considerando que este último sería un término aparentemente adoptado de la traducción del inglés del verbo to encrypt.[13] Así, se ha dicho que "encriptar", usada en el ámbito de la tecnología y de las comunicaciones, significa preparar un archivo o mensaje el cual solo podrá interpretarse si se dispone de una contraseña o clave.[14] Por otro lado, se ha comprendido "cifrar" como un verbo utilizado en la criptografía, el cual se usa como sinónimo de encriptar. El lenguaje general los ha diferenciado, otorgando a encriptar un sentido más amplio, el cual no siempre tiene como objetivo ocultar información, sino convertir un mensaje a un código tal que permitirá su posterior descifrado.[15]

Utilizaremos en adelante el vocablo "cifrado", entendido como una operación criptográfica reversible, que transforma datos significativos inicialmente sin proteger, conocidos como texto sin formato, en datos ilegibles, conocido como texto cifrado, utilizando una clave llamada clave de cifrado (Ewow, 2014). De forma más sencilla, se puede comprender como el proceso de convertir mensajes o información a una forma ilegible para todas aquellas personas que no sean su destinataria.[16]

El cifrado, al igual que el anonimato, no es una invención de nuestra época. Pueden ser rastreados sus orígenes a tiempos antiguos, fundamentalmente en África, Asia y Europa, normalmente asociado al intercambio de información asociado al comercio de mercaderías y de campañas militares. Incluso el antiguo Egipto existen señales de su utilización para ocultar el contenido de comunicaciones.[17] El desarrollo posterior está además asociado al aumento en formas y tecnologías de comunicación a distancia.

Así, las técnicas de cifrado informático usadas de forma más amplia en la actualidad tienen su origen en los Estados Unidos en la década de 1970, cuando IBM desarrolló el estándar a utilizar por la NSA en materia de seguridad digital.[18]

Si bien durante el siglo XX las técnicas de cifrado tuvieron un uso predominantemente militar, con el lanzamiento de la primera versión de PGP (Pretty Good Privacy) en 1991, por Phil Zimmermann, estas pasaron a estar disponibles para el el común de la población. Aun cuando ya existían servicios pagados para poder proteger las comunicaciones privadas de los usuarios, PGP es especialmente notable por dos motivos: es freeware y se convirtió en un estándar actual de seguridad en línea.[19] [20]

---

13 ACADEMIA DOMINICANA DE LA LENGUA. "Encriptar". Academia Dominicana de la Lengua. En línea, disponible en http://academia.org.do/encriptar/ [fecha de consulta: 03 de diciembre de 2015]

14 FUNDÉU BBVA. "Encriptar es Ocultar un Mensaje con una Clave". Fundéu BBVA. En línea, disponible en http://www.fundeu.es/recomendacion/encriptar-es-un-termino-valido/ [fecha de consulta: 03 de diciembre de 2015]

15 Ibíd., loc. cit.

16 Véase, para mayor detalle: SANS INSTITUTE. 2001. "History of Encryption". En línea, diponible en https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730 [fecha de consulta: 03 de diciembre de 2015] pp. 1-3.

17 Ibid., pp. 1-3.

18 Ibid., p. 5

19 Ibíd., p. 6.

20 Actualmente, PGP es software de pago, siendo su dueño la PGP Corporation. Dentro de las opciones actuales de software libre disponibles está GPG (Gnu Privacy Guard). GPG es una reescrituración y actualización de PGP, el cual usa un algoritmo de cifrado diferente de GPG para así asegurar su gratuidad. Actualmente, PGP permite la descarga de su software de forma gratuita solo para uso personal (el comercial es pagado), por otro lado, GPG permite su descarga sin costo tanto para uso personal como comercial. Extraído de DIFFERENCEBETWEEN.NET. Difference Between PGP and GPG. Differencebetween.net. En línea, disponible en http://www.differencebetween.net/technology/software-technology/difference-between-pgp-and-gpg/ [fecha de consulta: 31 de mayo de 2016]

Zimmermann (1999) señala que en la era de la información digital, la privacidad de las comunicaciones de los usuarios son más vulnerables que antes y para los gobiernos es más sencillo poder interceptarlas. En virtud de aquello, reconoce dos motivos fundamentales que llevaron a publicar PGP de forma gratuita: un proyecto de ley presentado por el Senado norteamericano en 1991 (Senate Bill 266), que pretendía obligar tanto a las empresas que prestaban servicios de comunicaciones digitales como a las manufactureras de equipos tecnológicos que permitieran comunicaciones seguras a instalar puertas de salida a tales equipos (backdoors), permitiendo así al gobierno tener acceso a los contenidos de esas comunicaciones, previa autorización judicial. Para Zimmermann, la masificación y popularización de tecnologías de cifrado le harán más difícil al gobierno de turno volver su uso ilegal (Zimmermann, 1999).

El segundo motivo apunta a que considera al cifrado como la única forma de no ceder que tiene el derecho a la privacidad ante las amenazas creadas a este en la era de la información digital.

Cabe señalar que Zimmermann ve la utilidad del software de cifrado en relación a los intentos de criminalización del uso de las técnicas de cifrado.

5.1. ¿CÓMO FUNCIONAN LAS TÉCNICAS ACTUALES DE CIFRADO?[21]

Al igual que al referirnos a anonimato, el cifrado se ha adaptado al correr del tiempo: desde el uso de ideogramas, dibujos o mensajeros que, en persona, llevaban un mensaje codificado en formato físico a su destinatario, hasta sistemas de llaves públicas y privadas digitales que permiten codificar el mensaje enviado por el emisor y ser decodificado únicamente por su receptor individualizado al inicio de dichas comunicaciones.

El uso del cifrado en las comunicaciones privadas entre personas se ha masificado, como pudimos ver, desde la década de 1990, y está presente en buena parte de las comunicaciones digitales. Con anterioridad, era principalmente utilizado en relación a la protección al acceso de información o enfocado en las transacciones realizadas a través de la red, entre servidores o bien entre personas y empresas, pero se ha extendido hasta las comunicaciones privadas sostenidas entre personas. En ellas nos concentramos en este análisis.

Un sistema de cifrado usado actualmente en diversas vías de comunicación es el sistema de llaves público-privada, conocido como cifrado de punto a punto o de extremo a extremo (end-to-end encryption). En términos sencillos, cada persona tiene su par de llaves, una pública (que conoce todo el mundo) y una privada (que conoce solo el propietario). El funcionamiento de este criptosistema se basa en el resguardo de la llave privada de cada uno y la distribución de la llave pública a los demás. De este modo, al enviar un mensaje cifrado, tenemos a dos personas: el emisor y el receptor. El emisor, para establecer comunicación cifrada con el receptor, debe conocer su llave pública, la cual puede ser enviada por él o puede extraerla de un directorio público de llaves. Así, al enviar un mensaje cifrado al receptor, la llave pública transforma el mensaje en uno aparentemente ilegible.

Entonces, ¿cómo el receptor puede leer lo que el emisor envía? Acá entra en funcionamiento la denominada llave privada, que es un archivo donde se encuentran los parámetros necesarios para descifrar el mensaje codificado en base a la llave pública del mismo receptor. Dada la naturaleza de los problemas matemáticos utilizados en el cifrado, romperlo por fuerza bruta es prácticamente imposible, puesto que requiere de operaciones de cómputo para adivinar los parámetros de cifrado que tomarían muchísimo tiempo. Como vemos, es finalmente el receptor (o mejor dicho, el poseedor de la llave privada) el único con la capacidad de descifrar el contenido del mensaje codificado.

---

21 Se agradece la colaboración de Martin Gubri e Israel Leiva en la redacción de este apartado.

Dentro de este esquema, eventualmente puede existir un tercer participante, un adversario que busca interceptar las comunicaciones entre el emisor y el receptor, usualmente durante su "trayecto". En caso que este tercero pueda capturar el mensaje, no podrá entenderlo, dado que estará compuesto por números, símbolos, letras, entre otros (sin un patrón evidente).

Por otro lado, existe el cifrado de comunicaciones con servidores de sitios web, identificado con HTTPS (Hypertext Transfer Protocol Secure). Este protocolo de cifrado crea una comunicación segura entre el usuario y el servidor en el cual el sitio está alojado, mediante un certificado SSL (Secure Sockets Layer) o TLS (Transport Layer Security, una versión posterior de SSL) asocia un nombre de dominio o un servidor a una organización y su ubicación. De este modo, al usar una conexión HTTPS, quien ingresa al sitio se asegura de que el contenido que ve en su pantalla es el sitio real, que no ha sufrido modificación alguna entre el transporte de información entre su equipo y el servidor, protegiendo así información sensible, como lo son contraseñas o cuentas bancarias. Es el servidor quien descifra el mensaje comunicado, no estando en poder de las partes el archivo que permite poder acceder al contenido.[22]

5.2. EL DEBATE ACTUAL SOBRE EL USO DE LAS TÉCNICAS DE CIFRADO

Actualmente, es posible encontrar freeware que permite sostener comunicaciones cifradas: aplicaciones para teléfonos como WhatsApp, Signal o Telegram; servicios de chat como Cryptocat o de ofuscación de chats con modo OTR (off-the-record); GPG Tools para facilitar el uso de PGP para enviar correos electrónicos cifrados o proteger el acceso a dispositivos de almacenamiento o archivos, entre otros. Destaca en este grupo, como expresión de la actual tendencia, la adopción de cifrado de punto a punto por parte de WhatsApp (propiedad de Facebook),[23] la aplicación de mensajería con la base de usuarios más grande del mundo, respecto a sus competidoras.[24]

Los sistemas operativos de computadores de escritorio y portátiles (macOS, Windows[25] y los sistemas operativos libres y de código abierto), como también de los teléfonos móviles inteligentes más populares del mercado (Android e iOS, en el caso de este último por defecto) entregan también la opción de cifrar la información contenida en sus sistemas de almacenamiento (como discos duros y discos de estado sólido). En este caso, el cifrado se mantiene sobre información estática; no obstante, ante cualquier intento de apoderamiento por un tercero que no cuente con una llave de descifrado, el contenido será virtualmente inaccesible.

---

22 Si el sistema de cifrado de llave privada responde a un cómo se cifra el mensaje, el cifrado de punto a punto responde a dónde se descifra. Así, una simple definición consta en Wired.com la cual indica que "(...) significa que los mensajes se cifran de manera tal que solo el receptor puede descifrarlo y no otra persona entre medio. En otras palabras, solo el computador al final de la cadena contiene la llave que permite descifrarlo y la compañía actúa como un mensajero analfabeto, el cual transporta el mensaje sin poder descifrarlo o leerlo por sí mismo". Definición extraída de GREENBERG, A. 2014. "Hacker Lexicon: What is End-to-End Encryption?". Wired.com. En línea, disponible en: http://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/ [fecha de consulta: 18 de enero de 2016] (la traducción es nuestra). Así, por ejemplo, Facebook no usa cifrado de punto a punto porque es el servidor el cual descifra el mensaje enviado para que así el receptor pueda leerlo, que es en la práctica cómo funcionan los mecanismos https. Por otro lado, si enviamos un correo electrónico cifrado con una herramienta como PGP Tools, no es nuestro servidor de correo quien descifra el contenido para el receptor, sino la llave privada que consta en un dispositivo que la contenga, por ejemplo, el laptop del receptor.

23 EL PAÍS. 2016. WhatsApp Activa el Cifrado de los Mensajes Para Todos los Usuarios. Elpaís.com. En línea, disponible en: http://tecnologia.elpais.com/tecnologia/2016/04/05/actualidad/1459875233_301649.html [fecha de consulta: 25 de abril de 2016]

24 EL COMERCIO. 2015. WhatsApp es la App de Mensajería Más Popular del 2015. Elcomercio.pe. En línea, disponible en: http://elcomercio.pe/tecnologia/actualidad/whatsapp-app-mensajeria-mas-popular-2015-noticia-1862521 [fecha de consulta: 25 de abril de 2016]

25 Sobre el cifrado de almacenamiento en Windows, ver Lee (2015).

El uso de técnicas de cifrado, tanto en el resguardo de información como en las comunicaciones privadas, tiene como propósito disminuir los riesgos de una comunicación cuyos contenidos puedan ser interceptados, riesgos que incluyen acceso a datos sensibles asociados a la ejecución de acciones como comprar por internet, recibir datos médicos, acceder a cuentas de redes sociales, cuenta bancaria y, en general, todo tipo de actividad en línea que suponga el acceso a información y cuya extracción ilegítima pueda revelar detalles sumamente precisos de la vida privada y generar perjuicios como consecuencia.

No obstante este panorama, no todos los usos de las técnicas de cifrado son igualmente aceptados. El uso de software de comunicaciones protegidas ha sido objeto de preocupación de los distintos gobiernos desde hace años, como recordamos, el lanzamiento de PGP en 1991 fue una respuesta a un proyecto de ley en los Estados Unidos que buscaba introducir vulnerabilidades en los servicios de comunicaciones y en los equipos necesarios para llevarlas a cabo. El combate al crimen organizado, estafas electrónicas, pornografía infantil, tráfico de sustancias ilícitas y a la actividad terrorista ha llevado, principalmente desde la década pasada, a incorporar modificaciones a la regulación de los servicios de telecomunicaciones, suponiendo intromisiones de alta intensidad al derecho a la privacidad de los usuarios.

Tal y como ha sucedido con el anonimato, el uso de cifrado no es algo que haya dejado indiferentes a las autoridades.

Al crear PGP en 1991, Zimmermann quiso crear conciencia sobre la existencia de suspicacias por parte de la esfera gubernamental, sobre todo por los sectores de seguridad nacional, en relación al uso de las técnicas de cifrado por parte de la ciudadanía. Allí, Zimmermann señaló que en el uso de herramientas de cifrado hay un juego de poder del cual el gobierno es consciente (Zimmermann, 1999).

En la presente década dicha discusión se revitalizó, como hemos visto con particular fuerza desde finales del año 2015, tras una serie de graves atentados terroristas acaecidos en Francia, California y Bélgica. El combate al crimen de alta peligrosidad ha influenciado la agenda legislativa a nivel global y el uso de técnicas de anonimato y cifrado suele ser asociado a la comisión de ilícitos altamente complejos. En miras de la seguridad social ante estas es que el debate sobre la legalidad y legitimación de la utilización de comunicaciones cifradas ha escalado con especial importancia.

Un reciente trabajo escrito por Phillip Rogaway (2015) de la Universidad de California Davis, aboga por un desarrollo de las tecnologías de comunicación consciente del daño que puede causarse a la ciudadanía con los avances de la ciencia. Indica que la misma tecnología que ha sentado las bases para la actual estructura de vigilancia estatal puede ayudar a revertir esta realidad para los usuarios de la red, con el uso del cifrado. Manifiesta su preocupación por la falta de ética y de real preocupación de la comunidad científica al investigar, quienes, por el bien del avance informático, han olvidado y parecen no estar interesados en las repercusiones que su trabajo tendrá en las vidas de cada uno de nosotros. En ese sentido, el autor manifiesta que la labor científica tiene consecuencias políticas, aun cuando los científicos no siempre estén plenamente conscientes de aquellas.

Tanto para Zimmermann como para Rogaway, es este juego de poder entre el Gobierno y la población civil donde está la verdadera discusión actual sobre el cifrado.

El deseo de incorporar vulnerabilidades en el software y hardware de comunicaciones fue denunciado en los Estados Unidos de América a inicios de los años ’90 con una serie de proyectos de ley como los primeros antecedentes que existen de intentos de debilitar el uso del cifrado por parte de la comunidad estatal de inteligencia. En la época eran bastante vehementes los argumentos utilizados, tanto por quienes luchaban en contra del acceso gubernamental a toda comunicación, como por quienes apoyaban el acceso a comunicaciones protegidas por parte del gobierno, al costo de introducir vulnerabilidades a los sistemas.

En 1994, en relación al famoso caso del Clipper Chip,[26] Dorothy Denning de la Universidad de Georgetown indicaba que de no implementarse una vulnerabilidad, "todas las comunicaciones transmitidas a través de la carretera de la información serían inmunes de interceptación legal. En un mundo amenazado por el crimen organizado internacionalmente, terrorismo y gobiernos corruptos, esta decisión sería insensata" (Levy, 1994).[27] Por otro lado, al consultarle a Phil Zimmermann por los usos ilegítimos del cifrado ante su idea de crear un teléfono protegido con PGP, respondió: "Estoy preocupado sobre qué podría pasar si se logran crear comunicaciones con seguridad ilimitada, pero también creo que en ello hay tremendos beneficios. Algunas cosas malas podrían suceder, pero el intercambio ("trade-off") valdría la pena. Tienes que mirar el panorama global" (Levy, 1994).[28]

Con las revelaciones de Edward Snowden a mediados de 2013 sobre la vigilancia de la NSA, la discusión sobre cifrado recobró renovadas fuerzas, con reiteración de los argumentos sobre seguridad nacional. Igualmente, llama la atención que el deseo de incorporar vulnerabilidades a los sistemas de comunicación privadas (para así posibilitar la entrega de aquellas al gobierno en caso de ser solicitadas) tampoco goza de especial novedad (McCullough, 2014). Si bien la iniciativa fue desechada en los años 90, actualmente ha sido reconsiderada por los servicios de seguridad, en tanto alegan que el cifrado ha complejizado su labor (Temple-Raston, 2015).

Si bien la controversia sobre el uso de cifrado ya estaba presente, los ataques terroristas acontecidos en París en el mes de noviembre de 2015 hicieron que la atención política volviera a estar altamente focalizada en el uso de técnicas de cifrado.[29] Para coordinar tales ataques suicidas, supuestamente habrían utilizado servicios de mensajería cifrados como WhatsApp y Telegram,[30] aun cuando ello fue eventualmente desmentido, puesto que se reveló que los atacantes usaron mensajería de texto (SMS) no cifrada.[31]

No obstante, en julio de 2015 el entonces director del FBI James Comey había señalado que el uso de cifrado, sobre todo en teléfonos inteligentes, ha supuesto una traba en el ejercicio de las funciones de dicho órgano. Argumentó que ni siquiera ellos disponen de las herramientas

---

26 El caso del chip Clipper ocurrió en los Estados Unidos en 1993. La administración del ex Presidente Bill Clinton buscaba incorporar una puerta trasera en los equipos de comunicaciones mediante un chip que sería instalado en ellos de modo tal que las fuerzas policiales pudieran tener acceso a las comunicaciones privadas llevadas a cabo por medio de estos, utilizando una copia de la llave que el Gobierno tendría almacenada para tales fines (key escrow). Aquella medida finalmente no prosperó, encontrando férrea resistencia. Extracto recogido de Higgins (2015).

27 "'If something like Clipper is not implemented', writes Dorothy E. Denning, a Georgetown University computer scientist, 'All communications on the information highway would be immune from lawful interception. In a world threatened by international organized crime, terrorism and rogue governments, this would be folly'".

28 "'I am worried about what might happen if unlimited security communications come about,' he admits. 'But I also think there are tremendous benefits. Some bad things would happen, but the trade-off would be worth it. You have to look at the big picture'".

29 Un resumen sobre la discusión puede encontrarse en Henn, S. y Selyukh, A., "After Paris Attacks, Encrypted Communication Is Back In Spotlight". NPR.org, 16 de noviembre de 2015. En línea, disponible en http://www.npr.org/sections/alltechconsidered/2015/11/16/456219061/after-paris-attacks-encrypted-communication-is-back-in-spotlight [fecha de consulta: 05 de enero de 2016]

30 PEREZ, E y PROKUPECZ, S. 2015. "First on CNN: Paris Attackers Likely Used Encrypted Apps, Officials Say". *CNN*. En línea, disponible en http://edition.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/ [fecha de consulta: 05 de enero de 2015]

31 Farivar, C., "Paris Police Find Phone With Unencrypted SMS Saying 'Let's go, We're Starting'". Ars Technica. En línea, disponible en: http://arstechnica.com/tech-policy/2015/11/paris-police-find-phone-with-unencrypted-sms-saying-lets-go-were-starting/ [fecha de consulta: 25 de abril de 2016]

necesarias para poder intervenir un cifrado fuerte.[32] El mismo exfuncionario, en discursos distintos resaltó el valor de la seguridad como bien público (en contraposición a la privacidad que es individual).

También indicó que el rápido avance tecnológico ha creado un desfase en la legislación vigente y ha dado espacio para la comisión no detectable de crímenes de alta peligrosidad. Punto central para la argumentación, es que las solicitudes a un tribunal en el marco de una investigación penal no tendrían valor alguno, en tanto el uso de cifrado no permita averiguar los datos críticos necesarios para el ente persecutor, puesto que se puede rastrear al criminal hasta cierto punto y luego es como si desapareciera (going dark) (Rogaway, 2015). Así, instan a la incorporación de mecanismos de acceso a los datos contenidos en los dispositivos de telecomunicaciones.

El sucesor de Comey en el FBI, Christopher Wray, no tardó en mantener la línea discursiva. Más recientemente, en octubre de 2017, dijo en un discurso público que el cifrado es un gran problema que impacta toda clase de investigaciones: narcóticos, tráfico de personas, contrainteligencia, pandillas, crimen organizado y explotación infantil. En la ocasión, también reveló que el FBI había fracasado en acceder al contenido de más de 6.900 teléfonos móviles por estar cifrado.[33]

Por otro lado, los defensores de las herramientas de cifrado (principalmente miembros de la sociedad civil y de las empresas de tecnología) han señalado posturas diferentes, en contra de la imposición de vulnerabilidades premeditadas. Así como presentamos los mecanismos más usuales de vulnerabilidades utilizadas para sortear las técnicas de cifrado fuerte, los argumentos en contra de la implementación de los anteriores y, en general, de la postura reticente al uso extendido de cifrado por la población pueden resumirse en los siguientes:

- No necesariamente ayuda al combate del crimen organizado: Como se suele decir en las discusiones relativas al uso ilegítimo de tecnologías, el cifrado, como herramienta, no es bueno ni malo en sí mismo, sino que la tecnología es neutra, y son los usuarios quienes la utilizan tanto para bien o para cometer ilícitos (Botero, 2015). Igualmente, lo que sucede en la red es solo una manifestación de lo que ocurre fuera de ella; por tanto, si se cometen ilícitos en el entorno digital, ellos han existido siempre y se seguirán realizando, incluso con o sin técnicas de cifrado, por otro lado, las mismas medidas que utilizan criminales en la red para no ser descubiertos son similares a las usadas por órganos encargados de mantener la seguridad ciudadana como por miembros de grupos vulnerables de la sociedad para protegerse del acoso que puede suponer que expresen su opinión en línea.[34]

- A su vez, se ha llamado la atención sobre el hecho de que no existen pruebas concluyentes que demuestren que el uso por parte de criminales de alta peligrosidad de tecnologías de cifrado sea una barrera infranqueable para la persecución criminal,[35] en tanto aunque se proteja el contenido del archivo enviado o de las comunicaciones, existen mucha información asociada al mensaje cifrado enviado que permite averiguar los datos necesarios que prueben una conexión entre individuos, pertenencia a ciertos grupos, hora, fecha, lugar y soporte usado para comunicarse, frecuencia de los contactos sostenidos, entre otro tipo de información.

---

32 TEMPLE-RASTON, D. 2015. op. cit.

33 Farivar, C., "FBI director: Unbreakable encryption is a 'huge, huge problem'", Ars Technica, 23 de octubre de 2017, disponible en https://arstechnica.com/tech-policy/2017/10/fbi-director-unbreakable-encryption-is-a-huge-huge-problem [fecha de consulta: 24 de octubre de 2017]

34 UNITED NATIONS, Human Rights Council. 2015. op. cit., p.6

35 Ibíd, op. cit., p. 15.

- Mucha de la información cifrada puede conocerse de todos modos sin tener que ser descifrada: Como declaró Moxie Marlinspike (fundador de Open-Whisper Systems, creadores de la herramienta de cifrado de software libre que utiliza WhatsApp para proteger sus comunicaciones) a NPR.com en 2015, la mayoría de los servicios comúnmente utilizados por los consumidores, protegen cifrando el contenido de los mensajes enviados por aquellos, mas no los metadatos, por tanto, si una red terrorista entabla contacto a través de una determinada plataforma, los servicios de inteligencia son capaces de detectarlo.

- En efecto, los análisis de metadatos permiten prever conductas con alto grado de certeza, revelando los patrones de comportamiento, puntos de vista, interacciones con otros y afiliaciones, considerándose que ella expone más al sujeto que el contenido mismo de las comunicaciones, el cual goza de mayor protección legal.[36] El cifrado no necesariamente protege todos los datos de la comunicación, así, aun cuando puede no ser posible conocer el mensaje enviado, la dirección IP de los equipos involucrados no siempre está oculta, por tanto, con ese solo dato terceros pueden recolectar una cantidad de información significativa.[37] También es necesario recordar que en algunos países del mundo (Chile incluido) existen normas que obligan a la retención de datos de comunicación, a través de los cuales se puede llegar a los usuarios de equipos conectados a la red (Díaz, 2017).

- Al crear deliberadamente una vulnerabilidad, ella puede afectar más servicios que los únicamente necesarios para la persecución penal: Al introducir algún tipo de debilidad en un sistema informático, esta vulnerabilidad no solo actúa a favor del gobierno interesado en mantener la seguridad de la población, sino que puede explotarla cualquiera que tenga las habilidades técnicas.[38] En esta postura también podemos encontrar a representantes de las más grandes empresas de tecnología.

  Para Tim Cook (CEO de Apple), una debilidad conscientemente introducida puede ser usada tanto por quienes tienen acceso legítimo como truhanes; a su vez, reconoce que los dispositivos Apple contienen muchos datos de su usuario, por tanto estos mismos tienen una expectativa de respeto de su privacidad al elegir tal compañía, creyendo que es bueno que el consumidor sepa y pueda controlar el flujo de tales datos.[39]

  El cifrado no solo protege archivos y mensajes. Como indicamos, resguardan también el tráfico comercial de los individuos y de grandes empresas también, así como secretos industriales y de propiedad intelectual (Greene, 2015). Es más, el mismo aparato gubernamental puede ser objeto de vulnerabilidades existentes en un sistema y la posterior exposición de la información allí contenida, caso ejemplar de lo cual es lo acontecido en diciembre de 2015 en Estados Unidos con las fallas de seguridad existentes dentro del firewall de Juniper Networks.[40] Por tanto, si un gobierno determinado exige a las empresas de tecnología (ya sea de manufacturación de equipos, empresas de telecomunicaciones o de software) introducir vulnerabilidades intencionalmente, ni ellos mismos se ven libres de los riesgos.

---

36 PRIVACY INTERNATIONAL. What is Metadata?. Privacyinternanal.org. En línea, disponible en: https://www.privacyinternational.org/node/53 [fecha de consulta: 11 de enero de 2016]

37 UNITED NATIONS, Human Rights Council. 2015. op. cit., pp. 4-5.

38 Ibíd, p. 4.

39 NPR, "Apple CEO Tim Cook: 'Privacy Is A Fundamental Human Right'. NPR.org, 1 de octubre de 2015, disponible en: http://www.npr.org/sections/alltechconsidered/2015/10/01/445026470/apple-ceo-tim-cook-privacy-is-a-fundamental-human-right [fecha de consulta: 11 de enero de 2016]

40 ZETTER, K., "Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors". Wired.com, 18 de diciembre de 2015, disponible en: http://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/ [fecha de consulta: 23 de octubre de 2017]

En efecto, la información sensible de la población requiere ser almacenada para prestar determinados servicios, como lo son los asociados a la salud, tramitación en línea ante servicios públicos o transacciones económicas, por señalar algunos ejemplos. La introducción de una vulnerabilidad puede abrir la ventana para el acceso ilegítimo a dichos datos sensibles, los cuales deben ser protegidos por los más altos estándares de seguridad en línea.

- La instalación de backdoors transgrede los derechos fundamentales del afectado. En el informe elaborado por David Kaye (2015), Relator Especial para la Libertad de Expresión del Consejo de Derechos Humanos de las Naciones Unidas, se destaca el rol que juega el anonimato y el cifrado, al permitir a los individuos ejercitar sus derechos a la libertad de opinión y expresión en la era digital.

  Específicamente respecto del cifrado, señala Kaye que, si bien no basta por sí solo, disminuyen los rastros que deja en su tráfico en la red. El cifrado trabaja creando una zona de seguridad que cautela el derecho a la libertad de expresión, incentivando así la navegación, opinión y desarrollo de ideas frente a amenazas externas.[41] Destaca el rol de los privados en la protección del derecho a la libertad de expresión en tanto su actual ejercicio, promoción y protección de las herramientas de cifrado. Así, indica que las empresas de telecomunicaciones, proveedores de servicios de internet, servicios de almacenamiento de información, encargados de motores de búsqueda, entre otros tipos de servicios tecnológicos que prestan, con su actuar y políticas de uso pueden promover o comprometer el uso de las técnicas de cifrado, en tanto estas compañías manejan grandes volúmenes de datos de sus usuarios, además de que las autoridades públicas se dirigen a aquellas solicitando tal información.[42]

  No solo en esta oportunidad se ha enfatizado en el especial peso que tienen los entes privados en el respeto de los derechos humanos, John Ruggie en 2011 elaboró un informe para Naciones Unidas en el cual se refirió al rol de aquellos en la protección, respeto y remedio sobre violaciones a estos. En este documento, Ruggie estableció como uno de los tres principios fundamentales de un marco que considere las tres aristas recién enunciadas "la obligación de las empresas de respetar los derechos humanos, lo que significa actuar con la debida diligencia para no vulnerar los derechos de terceros, y reparar las consecuencias negativas de sus actividades".[43]

- Kaye (2015) insiste en que toda restricción al cifrado debe ser en casos específicos, cumplimiento tal intromisión con los requisitos de legalidad, necesidad, idoneidad y proporcionalidad de la medida, siendo aprobada aquello por un juez. Igualmente, aboga porque la discusión sobre las limitaciones a este tipo de herramientas consideren los usos positivos, considerando que suele centrarse en los aspectos negativos. Finalmente, sugiere que los Estados deben promover el uso de técnicas de cifrado fuerte, para que así los individuos se sientan protegidos en su privacidad.[44]

---

41 Ibíd, p. 5.

42 Ibíd, p.10.

43 NACIONES UNIDAS, Consejo de Derechos Humanos. 2011. "Informe del Representante Especial del Secretario General para la Cuestión de los Derechos Humanos y las Empresas Transnacionales y Otras Empresas, John Ruggie". En línea, disponible en: http://www.ohchr.org/Documents/Issues/Business/A.HRC.14.27_sp.pdf [fecha de consulta: 13 de enero de 2016] p. 4.

44 UNITED NATIONS, Human Rights Council. 2015. op. cit., p. 19-20.

5.3. MECANISMOS DE DESCIFRADO FORZOSO Y ELUSIÓN DE CIFRADO

Como hemos mencionado, existen diversos mecanismos de elusión de cifrado o vulnerabilidades de los sistemas de cifrado. Ellos consisten en mecanismos que integran tanto componentes técnicos como institucionales, en que la ley juega un rol importante como facilitador del descifrado forzoso de comunicaciones o de información almacenada. Estos mecanismos pueden dividirse normalmente en los siguientes:

- Puertas traseras (backdoors): Se definen como un método para sortear la autenticación u otro tipo de control de seguridad necesaria para acceder a un sistema computacional o a los datos contenidos en este. Pueden existir tanto a nivel de sistema operativo, en un algoritmo de cifrado o dentro de una aplicación (Wysopal et al, 2008). Estas puertas permiten poder acceder al sistema o información contenida en él de forma local o remota.[45] Se ha dicho que en Estados Unidos como en el Reino Unido actualmente se busca introducir estos mecanismos para poder descifrar comunicaciones cifradas (Leonard, 2015).

  Este método en particular ha sido objeto de críticas, en tanto introducir una vulnerabilidad de este estilo no discrimina entre accesos legítimos e ilegítimos, ni entre accesos por el gobierno o por terceros. La debilidad creada puede ser aprovechada por cualquiera, en tanto no reconoce la finalidad de la intrusión al sistema.

- Copia de la llave privada: A diferencia de una puerta trasera, en la cual se accede de forma subrepticia a un sistema computacional, existen otros métodos en los cuales la entrada es directa y frontal. Dentro de esta forma de intervenir comunicaciones y archivos cifrados, las dos formas más comunes son la obligación legal de entrega de la llave privada en caso de ser solicitada (key disclosure) y el depósito de claves (key escrow).

  El primero de estos métodos (key disclosure) consiste en la obligación contenida en una ley que obliga a un individuo a revelar su llave privada a los entes encargados de la persecución criminal en caso que aquellos la soliciten, cumpliendo con el procedimiento legalmente establecido para aquello; generalmente, previa autorización judicial (Lin, 2010).

  Numerosos países han legislado sobre el tema, lo cual ha sido objeto de críticas, especialmente dirigidas a la intensidad de la intrusión a los derechos del sujeto a quien se le exige la entrega de esta clave. Las medidas intrusivas suelen estar delimitadas por los contornos que el juez establece en su autorización, donde (idealmente) debe señalarse con precisión sobre qué piezas específicas recae la medida, minimizando así la vulneración en los derechos de este individuo, en razón de un test de proporcionalidad. Así, solicitar una llave privada no es lo mismo que exigir la entrega de un documento puesto que, por la naturaleza de la misma, esta implica dar acceso a todos los archivos y comunicaciones protegidas, superando todo margen de proporcionalidad (Clemens, 2004).

  El segundo mecanismo, key escrow, ha sido definido como un proceso en el cual algo (como un documento o una llave privada) es entregado a un tercero, quien solo puede autorizar el acceso al archivo entregado previo cumplimiento de las condiciones impuestas para aquello.[46] Normalmente, este mecanismo importa la entrega de una

---

45 PC MAGAZINE ENCYCLOPEDIA. "Definition of Back Door". PC Magazine.com. En línea, disponible en http://www.pcmag.com/encyclopedia/term/38339/back-door [fecha de consulta: 05 de enero de 2016]

46 JUST, M. 2011. Key Escrow Definition en JAJODIAL, S y VAN TILBORG, H (editores) 2011. "Encyclopedia of Cryptography and Security". Estados Unidos, Springer USA, segunda edición, p. 681.

copia de la llave privada a las agencias de seguridad públicas o que las empresas de telecomunicaciones mantengan una, solo revelándola en caso de existir una investigación penal en contra del sujeto. Un buen ejemplo es el "Chip Clipper" en los años 90, al cual ya nos hemos referido.

El discurso de la NSA estadounidense estaba dirigido en dirección a obtener este tipo de ingreso a las comunicaciones cifradas, señalando que no se desea una puerta trasera, sino una frontal que contenga múltiples candados de gran envergadura (cfr. Gellman y Nakashima, 2015). Por otro lado, se ha dicho que este tipo de soluciones son demasiado complejas de ejecutar y bordean lo contradictorias, además de resaltar que la complejidad es enemiga de la seguridad: en tanto más complejo es el sistema, este contendrá más imperfecciones que pueden ser aprovechadas por terceros que busquen accesos ilegítimos (Abelson, 2015).

Para David Kaye (2015), los mecanismos de key escrow igualmente presentan una serie de problemas a tener en cuenta, principalmente vinculados a la confianza en el depositario de la llave (que puede ser el gobierno o un tercero confiable). Este sistema depende de la integridad de quien almacena la llave, de la seguridad del archivo de llaves, que puede ser objeto de ataques externos tratando de acceder de forma ilegítima a ese archivo. Sobre las soluciones del tipo key disclosure, Kaye expresa que un mecanismo menos lesivo al principio de proporcionalidad sería que las autoridades (previa autorización judicial) soliciten al sujeto descifrar el o los mensajes en particular cuyo contenido necesitan conocer, en vez de solicitar la llave que permite tener acceso total.

- Fuerza bruta: Es el método más rudimentario, el cual consiste en intentar todas las combinaciones posibles hasta dar con la que permite dar acceso al sistema, usualmente mediante mecanismos que automatizan cada intento variando las combinaciones. En el caso de contraseñas, por tanto, en caso de que las utilizadas sean débiles (muy cortas o de fácil deducción son mucho más fácil de adivinar que contraseñas "fuertes".[47]

  Respecto de la llave privada, la situación es similar, puesto que al igual que una contraseña, se trata de una secuencia de caracteres. Originalmente, como ya vimos, las secuencias solían ser más reducidas, por lo cual para poder velar por la protección de esta clave, es que se ha optado por incrementar de forma sostenida su extensión y lo aleatorio de su composición. No obstante, por mucho que la estructura se haya complejizado, no las hace invulnerables. En efecto, el cifrado en su esencia sigue siendo una operación matemática y los computadores cada vez son más poderosos, aumentando su capacidad para poder descifrar una clave privada.[48]

  Específicamente, dentro de los sistemas de cifrados de llaves pública-privada, existe un algoritmo para crear nuevas llaves, por lo mismo, si se descubre el anterior, se simplifica el proceso de descifrar la llave privada por esta vía (Blumenthal, 2007).

- Malware:[49] Contracción de malicious software; es un concepto genérico que engloba una serie de programas diseñados para alterar o denegar las operaciones del siste-

---

47 Un sencillo ejemplo de cómo crear contraseñas fuertes puede ser encontrado en González (2014).

48 Véase, por ejemplo: "Brute-Force Attacks Explained: How All Encryption is Vulnerable". How-to-Geek.com. En línea, disponible en: http://www.howtogeek.com/166832/brute-force-attacks-explained-how-all-encryption-is-vulnerable/ [fecha de consulta: 07 de enero de 2016]

49 Definición extraída de USLEGAL. "Malware Law & Legal Definition". USlegal.com. En línea, disponible en: http://definitions.uslegal.com/m/malware/ [fecha de consulta: 07 de enero de 2016]

ma, recolectar información del usuario o permitir la explotación de otros servicios, obtener acceso no autorizado a los recursos del sistema y otro tipo de comportamiento abusivo. El malware interfiere con las funciones normales de un sistema computacional o envía a través de la red datos del usuario a terceros no autorizados. Dentro del concepto de malware se engloban una serie de software nocivos como los virus, troyanos, gusanos, software espía, secuestro de navegadores (browser hijacking), entre otros.

Bajo esta definición es que es posible vislumbrar cómo puede ser obtenido el archivo que contiene la llave privada en un sistema computacional y, en realidad, puede accederse a cualquier comunicación privada o archivo que estén resguardados por un fuerte cifrado. Así por ejemplo, si se requiere ingresar una contraseña para ingresar a una cuenta o para ver un archivo protegido o se quiere ver el contenido de las comunicaciones sostenidos por un servicio de mensajería de texto cifrado, basta con la instalación de un software de keylogging. Luego, habiendo desbloqueado el archivo puede copiarse y enviarse a otros dispositivos.

6. LA RELACIÓN ENTRE ANONIMATO Y CIFRADO

6.1. LA RELACIÓN TÉCNICA ENTRE ANONIMATO Y CIFRADO[50]

Por defecto, un mensaje cifrado no es anónimo. El cifrado permite sostener comunicaciones seguras sin que un tercero ajeno pueda entender el mensaje transmitido. Y, en caso que pueda interceptar el mensaje, no podrá decodificarlo. No obstante, si bien el mensaje le será ilegible, este tercero de todos modos puede conocer los metadatos asociados a este contacto entre las partes.

En efecto, lo anterior se debe a la misma naturaleza de las redes de computadores las cuales, básicamente, son conjunto de varios equipos conectados que se envían entre sí pequeñas piezas de información o "paquetes", transportando aquellas de un lugar a otro. La red requiere saber hacia dónde se dirige el mensaje y de dónde proviene para así poder ser enviado. Quienes usan software y aplicaciones habituales de comunicación y mensajería como GnuPG, chat off-the-record, Signal u otro, solo ven protegido el contenido de lo comunicado mediante cifrado de punto a punto, pero tales servicios no ofrecen un resguardo en el anonimato.

Debido a esto, si un tercero está vigilando la red, aun cuando no puede descifrar ni acceder al contenido mismo del mensaje enviado, será capaz de averiguar una serie de datos conexos a tal comunicación, como lo son: quienes se comunican, el número de mensajes enviados, la hora y fecha de emisión, incluso el peso aproximado de cada uno de aquellos y, usualmente, podrá averiguar también a través de software se sostuvo el contacto entre las partes.

Al igual que en el caso de uso de un método end-to-end, el cifrado vía protocolo HTTPS no asegura anonimato, sino que solo protege de terceros el conocimiento de estos datos altamente sensibles. En primer lugar, el servidor es capaz de identificar a la persona que accede al mismo para enviar mensajes, puesto que conoce los metadatos enunciados anteriormente, pero además toda la información que quien busca usar el servicio debe entregar para poder crear una cuenta en el mismo, y otro cúmulo de información que puede recolectar en caso de usar las versiones móviles (geolocalización, registro de números telefónicos, archivos almacenados en el dispositivo, entre otros).

Por otro lado, el servidor mismo puede contener métodos de rastreo en línea (website visitor trackers), los cuales pueden ser definidos como contenido externo a un sitio web, pero que se encuentran incorporados al mismo, los cuales identifican el navegador que utiliza el usuario, además de las páginas que este visita. Normalmente, son usados para conocer quienes visitan un sitio en particular con fines de venta de publicidad dirigida en redes sociales o para identificar el contenido favorito de quienes visitan un sitio, para así planificar la elaboración de contenidos en virtud de las preferencias de los navegantes. Ni siquiera las comunicaciones seguras que puedan sostenerse en estos sitios pueden proteger al usuario de la totalidad de estos trackers.

Finalmente, está la noción de huella digital. Esta permite que cada vez que visitamos un sitio, nuestro navegador y las extensiones del mismo pueden filtrar información, así, nuestra combinación de sistema operativo, navegador, extensiones, programas y hábitos dan cuenta de nuestra identidad (Gilbertson, 2010).

No obstante, existen formas de navegar y comunicarse de forma cifrada y anónima, siendo la red Tor (The Onion Relay network) el mejor ejemplo. Tor cifra la información a ser enviada en varias capas, y luego la envía a través de una red de servidores alrededor del mundo (la red Tor), en donde cada servidor descifra una capa y pasa la información al siguiente, sabiendo solamente quién le envió la información y a quién debe enviársela, pero no el trayecto completo. Es el servidor final (o de salida) el que descifra la última capa y conoce el destino final de la comunicación. Así, ningún servidor en el trayecto conoce el origen y el destino a la vez.

---

50 Se agradece la colaboración en la elaboración de esta sección a Martin Gubri y a Israel Leiva.

Cabe notar que Tor solamente cifra la comunicación mientras ella ocurre dentro de la red Tor, no antes ni después. Una debilidad de esto es que si el tráfico no está cifrado desde el principio (como en las webs con HTTPS), el servidor de salida puede analizar el contenido e intentar desanonimizar al usuario. Por otro lado, utilizar Tor permite ocultar el lugar de origen de la comunicación, pero eso no es suficiente para ser completamente anónimo. Para ello se deben tomar resguardos adicionales como utilizar protocolos seguros, no repetir patrones de navegación y evitar tecnologías propensas a ser explotables por hackers (como Adobe Flash), entre otras medidas. Sin perjuicio de lo anterior, Tor no está libre de fallos, reportándose que, por diseño, es posible identificar al usuario de la red tanto en los nodos de salida como de entrada (Koebler, 2014).

6.2. LA RELACIÓN ENTRE ANONIMATO, CIFRADO Y DERECHOS FUNDAMENTALES

David Kaye (2015) identifica al anonimato y al cifrado como los medios idóneos para la seguridad en línea, puesto que dotan al individuo de métodos para proteger su privacidad, empoderándolos a navegar, leer, desarrollar y compartir sus opiniones e información sin interferencias, además de permitir a periodistas, organizaciones de la sociedad civil, miembros de grupos étnicos o religiosos, a quienes son perseguidos por su orientación sexual o identidad de género, activistas, investigadores, artistas y a la sociedad toda a ejercitar su derecho a la libertad de expresión y opinión.

Los Relatores Especiales para la Libertad de Expresión de Naciones Unidas y de la Comisión Interamericana de Derechos Humanos se han referido con anterioridad a la vigilancia masiva y sus repercusiones en los derechos de los usuarios de tecnología.

En la declaración conjunta del año 2013, sobre programas de vigilancia y su impacto en la libertad de expresión, los entonces relatores especiales manifestaron su preocupación sobre el efecto nocivo que el monitoreo en línea puede tener sobre estos dos derechos, dado su carácter sumamente invasivo, enfatizando la gran capacidad técnica de la cual disponen actualmente los Estados para vigilar comunicaciones privadas, el importante rol que desempeña internet en el actual ejercicio de derechos humanos y como el tráfico a través de la red ha supuesto que allí se acumule una gran cantidad de datos de las personas, los que se pueden sistematizar y revelar[51] tanto o más de los sujetos que el contenido mismo de lo que comunican. Es esto último por lo cual la protección del anonimato en línea es relevante.

Como explicamos anteriormente, anonimato y cifrado no solo van de la mano desde un punto de vista eminentemente técnico, sino también de protección de derechos. La Relatoría Especial para la Libertad de Expresión de la CIDH identifica como políticas idóneas para proteger a los derechos a la privacidad y de libertad de expresión en internet tanto a las protección de los datos personales como del discurso anónimo,[52] pero no solamente se requiere de anonimato en la participación democrática moderna –en los términos de la Relatoría–, sino que actualmente, tal y como vislumbra Kaye, también es necesario que las comunicaciones se encuentren resguardadas.

No obstante, si bien en la publicación de 2013 y en la declaración conjunta realizada no hay referencias al cifrado, en el Informe Anual de la Relatoría de la CIDH del año 2014 pueden encontrarse menciones indirectas al cifrado, especialmente respecto a los programas de vigilancia y reserva de fuente periodística.

---

51 NACIONES UNIDAS, ORGANIZACIÓN ESTADOS AMERICANOS. 2013. Declaración Conjunta Sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión. En línea, disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927 [fecha de consulta: 29 de enero 2016]

52 COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS. 2013. op. cit, p. 63.

Allí la Relatoría expresó su preocupación por la existencia de este tipo de programas en países de la región y el serio menoscabo que ellos generan a los derechos humanos, recomendando que los Estados establezcan límites a la potestad para vigilar las comunicaciones privadas y que, al ponerse en práctica medidas que supongan vigilancia, se respeten los principios de necesidad y proporcionalidad. Además, se recomienda que pongan a acceso del público información sobre los programas de vigilancia, para garantizar que no sean utilizados de forma arbitraria. Finalmente, sugiere que no se sanciones a periodistas, integrantes de los medios de comunicación o miembros de la sociedad civil que hagan pública la información que obtengan sobre este tipo de programas.[53]

Lo anterior da cuenta que el anonimato no protege por sí solo los derechos a la privacidad y libertad de expresión ante vigilancia masiva. Por ello que el cifrado es necesario para resguardar los mensajes enviados entre emisores y receptores, sobre todo en caso de que aquellos pertenezcan a estos grupos especialmente vulnerables, enunciados al comienzo. En este sentido se pronunció Bruce Schneier,[54] indicando que el cifrado es la herramienta más importante que existe en la actualidad para proteger la privacidad de las personas y que debe ser usado por toda la población. El uso generalizado del cifrado hace menos conspicuo a quien lo usa para resguardar su integridad.

En caso que no sea el mensaje, sino el emisor o el receptor quien necesita protegerse, el anonimato toma una segunda dimensión que debe ser protegida, la cual va dirigida al individuo en tanto quiere ocultar quién es.

En este sentido, el anonimato se ha alzado a lo largo de la historia como un método para expresar opiniones poco populares, como lo son manifestarse acerca de una opción de vida minoritaria e informarse sobre ella (Shaik, 2014), emitir una opinión política controvertida (Simpson, 2015), denunciar irregularidades (Véliz, 2013), manifestarse artísticamente sin miedo a que la atención de la crítica se dirija al autor sino a la obra,[55] y el desarrollo de la actividad periodística (García, 2004).

No obstante, las comunicaciones sostenidas entre miembros pertenecientes a estos grupos, el periodista y su fuente, el denunciante (whistleblower) y la entidad a la cual denuncia, los mensajes enviados entre la persona real del artista y su editor, deben ser protegidas por un cifrado fuerte, puesto que de conocerse o descifrar la identidad del denunciante como resultado de un análisis de su actividad en línea y cruces de información hará que se pierda toda la utilidad del anonimato, concepto que ya vimos que incluye muchos datos aparte del nombre y descritos por Marx (2001).

Es así como cifrado y anonimato, en conjunto, son las herramientas más aptas de las cuales disponemos actualmente para poder ejercitar y proteger nuestros derechos a la privacidad y libertad de expresión en la era de las comunicaciones digitales.

---

53 ORGANIZACIÓN DE ESTADOS AMERICANOS. Comisión Interamericana de Derechos Humanos. 2015. Informe Anual de la Comisión Interamericana de Derechos Humanos 2014. Informe Anual de la Relatoría Especial para la Libertad de Expresión. En línea, disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/anuales/Informe%20Anual%202014.pdf [fecha de consulta: 28 de enero de 2016] p. 435.

54 PRIVACY INTERNATIONAL. 2015. Securing Safe Spaces Online: Encryption, Online Anonymity and Human Rights. En línea, disponible en: https://www.privacyinternational.org/sites/default/files/Securing%20Safe%20Spaces%20Online_0.pdf [fecha de consulta: 29 de enero de 2016] pp. 3-4.

55 Véase el ejemplo reciente de la popular autora J.K. Rowling en: INGRAHAM, N., 'Harry Potter' Author J.K. Rowling Assumed Male Identity to Secretly Release a Detective Novel. The Verge, 14 de julio de 2013, disponible en: http://www.theverge.com/2013/7/14/4522398/harry-potter-author-j-k-rowling-secretly-releases-detective-novel [fecha de consulta: 29 de enero de 2016]

6. REGULACIÓN LEGAL DEL ANONIMATO Y EL CIFRADO

6.1. DERECHOS HUMANOS Y REGULACIÓN DE LAS COMUNICACIONES DIGITALES

El citado informe de la Relatoría Especial para la Libertad de Expresión de la CIDH referido al año 2014 y lanzado en 2015 enuncia su opinión al respecto, expresando su preocupación sobre los intentos de varios Estados latinoamericanos dirigidos a regular uno o más aspectos relacionados al acceso y uso de internet, en tanto algunos esos intentos vulneran derechos fundamentales. También llama la atención sobre los intentos por normar esta forma de telecomunicación usando estrategias propias de otras, como la telefonía, pasando por alto sus características únicas.[56]

Así, el informe sugiere a los Estados latinoamericanos tener en cuenta los siguientes puntos al elaborar iniciativas normativas referentes a la red:

- Abstenerse de aplicar a internet enfoques de reglamentación desarrollados para otros medios de comunicación, y diseñar un marco normativo alternativo y específico para este medio, atendiendo a sus particularidades, de conformidad con los estándares internacionales al respecto.
- Incentivar la autorregulación como herramienta efectiva a la hora de abordar las expresiones injuriosas que puedan emitirse a través de internet.
- Proteger a los intermediarios en internet y a quienes brindan servicios técnicos respecto de cualquier responsabilidad por los contenidos generados por terceros y que se difundan a través de los servicios que ellos prestan.
- Promover el acceso universal a internet para garantizar el disfrute universal y efectivo del derecho a la libertad de expresión por este medio.
- Garantizar que el tratamiento de datos y el tráfico de internet no sea objeto de ningún tipo de discriminación en función de factores tales como dispositivos, contenido, autor, origen o destino del material, servicio o aplicación, en conformidad al principio de neutralidad en la red.

El Consejo de Derechos Humanos de Naciones Unidas, a través del informe de Ruggie (2015), ha resaltado que el sector privado cumple, al igual que la esfera pública, un rol en esta labor protectora, por tanto debiera adecuar sus prácticas al respeto de los derechos humanos y velar por dicho respeto. Por ello, la empresas de telecomunicaciones no solo deben observar el cumplimiento y respeto de los derechos y libertades fundamentales en virtud de los mandatos destinados a dicho fin en la regulación sectorial elaborada por los organismos públicos competentes, sino que también de plena iniciativa como parte de su funcionamiento.[57]

En esta línea, se ha sostenido que la autorregulación en el ámbito de internet es la opción más viable de regular a la red.[58] Bajo un modelo autorregulatorio, las empresas de telecomunicaciones elaboran las prácticas que estimen convenientes para proteger los derechos de sus usuarios, pudiendo incluso superar el estándar legalmente exigido y no generar ineficiencias propias de una sobre regulación (Castro, 2011). No obstante, en relación con el derecho a la privacidad, se

---

56 COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, Relatoría Especial para la Libertad de Expresión. 2015. op. cit., p. 434.

57 NACIONES UNIDAS, Consejo de Derechos Humanos. 2011. op. cit., pp. 3-6.

58 Véase, por ejemplo, THE GUARDIAN. 2008. Harmful Content on the Internet: Self-Regulation is the Best Way Forward. The Guardian. En línea, disponible en: http://www.theguardian.com/media/organgrinder/2008/aug/01/post88 [fecha de consulta: 01 de febrero de 2016]

ha propuesto la adopción de un modelo corregulatorio, en tanto la autorregulación no ha dado resultados positivos, puesto que las compañías de tecnología cada vez recolectan más datos de sus usuarios.[59]

Sea cual sea la opción tomada por los gobiernos para regular la red (autorregulación, regulación estatal o modelos intermedios), hay dos ideas básicas que deben tenerse en cuenta y respetarse. La primera de ellas, como han indicado distintos informes de relatorías especiales, es que internet difiere de otros métodos clásicos de comunicación como lo son la radio o la telefonía y que dichas características especiales deben ser respetadas y atendidas en caso de dictar leyes y elaborar normativa administrativa al respecto. Moya (2003) enuncia tales características:

- Global: Se puede acceder a ella desde cualquier parte del mundo.
- Descentralizada: No tiene dueño, representante legal ni gerente, puesto que en su diseño se encuentra la idea clave de que en ella se pueda trabajar descentralizadamente, sin ningún tipo de restricciones ni ataduras. Igualmente, Moya señala que, dentro de esta característica, se incluye que internet es un objeto libre de estructuras jerárquicas de vigilancia y control.
- Abierta: Cualquier persona con acceso a internet puede generar contenidos, puesto que presenta escasas barreras de acceso.
- Grande: Dada su alta capacidad de almacenamiento de información.
- Interactiva: El diseño mismo de la red -bidireccional- apunta a que todos sus usuarios pueden ser emisores y receptores de la información allí vertida, modificando los esquemas tradicionales de comunicación.
- Controlada por el usuario: El usuario es libre de escoger los contenidos a los cuales quiere acceder y compartir.
- Independiente de la infraestructura: No está ligado a ninguna infraestructura que no sea la red física compuesta por cables, antenas y satélites, estando así lejos de un control gubernamental efectivo.

Por otro lado, los Estados tienen entre sus deberes la protección de los derechos humanos de quienes usan las tecnologías digitales, teniendo en cuenta tal resguardo a la hora de legislar sobre internet, lo cual se hace urgente considerando la tendencia global a elaborar normativa que transgrede tales derechos en pos de proteger otros bienes jurídicos, como la seguridad pública. Así, al regular internet, se debe cuidar no alterar los principios anteriormente enunciados, propiciando que los individuos generen contenido y puedan expresarse, además de respetar la naturaleza de internet como una red independiente, abierta y descentralizada.

6.2. PANORAMA REGIONAL DE LA REGULACIÓN DE ANONIMATO Y CIFRADO

A nivel regional, existen diversas normas que contienen disposiciones referidas a cifrado y anonimato, las cuales se concentran generalmente en los textos constitucionales, en las leyes de protección de datos personales, en las leyes de telecomunicaciones, en las leyes de registro móvil y de tráfico en internet, en las leyes que regulan medios de comunicación en la legislación procesal penal y en las que crean algún registro para uso de instituciones públicas, como las tarjetas de transporte o similares. A continuación se presentarán una serie de esquemas que exponen las normas aplicables a los dos temas que son objeto de este informe.

---

59 Véase como ejemplo HIRSCH (2011).

RESERVA DE IDENTIDAD

La reserva de fuentes está consagrada en el principio Nº 8 de la Declaración de Principios de la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos en los siguientes términos: "Todo comunicador social tiene derecho a la reserva de sus fuentes de información, apuntes y archivos personales y profesionales".[60] El contenido de la reserva de fuentes está dado por guardar reserva sobre los siguientes hechos: sobre la existencia de una determinada información, su contenido, el origen o la fuente de la misma, o la manera como obtuvo dicha información.[61]

Resguardo constitucional: En las Constituciones latinoamericanas no existe una protección amplia al anonimato en todas las circunstancias. No obstante, las cartas fundamentales de Argentina, Brasil y Paraguay otorgan resguardo constitucional a la protección de fuentes informativas, siendo esta la única manifestación del mismo.

En Argentina, el artículo 43 de la Constitución, en relación a la regulación de la acción de amparo, dispone que si bien esta acción puede interponerse para conocer los datos personales contenidos en registros públicos o privados, en ningún caso puede afectar la reserva de fuentes periodísticas.

A pesar de prohibir el anonimato, la Constitución Federal Brasileña lo acepta única y excepcionalmente en el caso de la reserva de fuentes periodísticas. Así, en el título II, capítulo I, artículo 5 XIV establece que el acceso a la información es garantizado a todos y la confidencialidad de la fuente será resguardada, cada vez que lo anterior sea necesario para el desempeño de la labor profesional.

Paraguay resguarda constitucionalmente la reserva de fuentes en el artículo 29 de su carta fundamental, el cual establece que el ejercicio del periodismo, en cualquiera de sus formas, es libre y no está sujeto a autorización previa. Prosigue señalando que los periodistas de los medios masivos de comunicación social en cumplimiento de sus funciones, no serán obligados a actuar contra los dictados de su conciencia ni a revelar sus fuentes de información.

La Constitución ecuatoriana, en su artículo 20, dispone que el Estado garantizará la cláusula de conciencia a toda persona, y el secreto profesional y la reserva de la fuente a quienes informen, emitan sus opiniones a través de los medios u otras formas de comunicación, o laboren en cualquier actividad de comunicación. La modificación al reglamento de infracciones administrativas de la ley orgánica de comunicación de 2015, establece en su artículo quinto que los órganos públicos y particulares que deban entregar información a la Superintendencia de la Información y de la Comunicación en las investigaciones están obligados a hacer tal entrega en las denuncias que aquella tramite, incluso la información que está sujeta a reserva, introduciendo una excepción enorme a la garantía constitucional a la reserva de fuentes.

Protección al anonimato en leyes de prensa: Si bien no todos los países de la región le otorgan respaldo constitucional al anonimato a nivel constitucional, si las hay a nivel legal. Chile, Panamá, Uruguay y Venezuela se enmarcan en este modelo. El caso chileno será tratado en el apartado siguiente.

La Ley Nº 22 de 2005 de Paraguay dispone en el artículo 4 que el responsable de la información o la noticia difundida por los medios de comunicación social no estará obligado a revelar la identidad de su fuente, sin perjuicio de las responsabilidades en que incurra por sus afirmaciones.

---

60 ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Comisión Interamericana de Derechos Humanos. Declaración Sobre Principios Sobre Libertad de Expresión. En línea, disponible en: https://www.cidh.oas.org/basicos/basicos13.htm [fecha de consulta: 02 de mayo de 2016]

61 COLOMBIA. Corte Constitucional. 2009. Sentencia T-298/09 Deberes Constitucionales de los Medios de Comunicación. corteconstitucional.gov.co. En línea, disponible en: http://www.corteconstitucional.gov.co/relatoria/2009/T-298-09.htm [fecha de consulta: 02 de mayo de 2016] El destacado es nuestro.

La Ley Nº 16.099 del año 2000 de Uruguay que establece normativa referente a la libertad de expresión, opinión y difusión, en la parte final de su primer artículo contempla la reserva de fuentes informativas anónimas en los siguientes términos: "Los periodistas tendrán el derecho a ampararse en el secreto profesional respecto, a las fuentes de información de las noticias que difundan en los medios de comunicación".

Respecto a los denunciantes, Perú concede protección específica, pero a nivel administrativo y solo respecto de denuncias en el sector público, en términos no distantes de los de la Ley de Transparencia en Chile. El resto de los países contempla un grado de protección indirecto, el cual puede ser encontrado en legislación procesal penal.

Protección al anonimato en legislación sobre protección de datos personales: Las leyes de protección de datos personales de algunos países de la región obligan a llevar a cabo procesos de anonimización de los datos personales recabados.

Generalmente, es posible encontrar estas disposiciones en las normativas más actualizadas y dictadas dentro de los últimos diez años. Se trata no tanto de un ocultamiento de identidad como de la disociación de información de las personas a quienes concierne.

Como ejemplo, el artículo 28 de la Ley Nº 25.326 sobre Protección de Datos Personales de Argentina, al referirse a los trabajos de encuestas de opinión, mediciones y estadísticas, prospección de mercado, investigaciones científicas o médicas y otras actividades análogas, indica que no le serán aplicables esta ley protectora en tanto dicha información no pueda ser atribuible a persona determinada o determinable. Ahora, en aquellos casos en que no resulte posible el anonimato en el proceso de recolección informativa, se debe aplicar la técnica de la disociación, para que así no se pueda identificar a ninguna persona.

De modo similar, la ley de datos personales peruana incorpora la obligatoriedad de anonimizar datos personales en caso de usarles con una finalidad distinta a la original.

Regulación que prohíbe el anonimato.

En este apartado se profundizará en los distintos países de la región, analizando las leyes vigentes que no permitan su ejercicio. Dentro de las fuentes formales del derecho en los países de la región, podemos encontrar los siguientes obstáculos al anonimato.

Prohibición expresa del anonimato:

La Constitución Federal Brasileña en su artículo 5º, al tratar la libertad de expresión, señala que "es libre la manifestación del pensamiento, quedando prohibido el anonimato".

El artículo 57 de la Constitución de la República Bolivariana de Venezuela señala que: "Toda persona tiene derecho a expresar libremente sus pensamientos, sus ideas u opiniones de viva voz, por escrito o mediante cualquier otra forma de expresión, y de hacer uso para ello de cualquier medio de comunicación y difusión, sin que pueda establecerse censura. Quien haga uso de este derecho asume plena responsabilidad por todo lo expresado. No se permite el anonimato, ni la propaganda de guerra, ni los mensajes discriminatorios, ni los que promuevan la intolerancia religiosa".

La ley venezolana de responsabilidad social en radio, televisión y medios electrónicos de 2004 contempla en su artículo 29, donde están las conductas prohibidas por esta ley, así como su sanción en específico. Dentro de las infracciones se considera la difusión de mensajes anónimos.

Ecuador, en el artículo 20 de la Ley Orgánica de Comunicaciones de 2013, contempla que los comentarios formulados al pie de las publicaciones electrónicas de los medios de comunicación en internet

deben contar con registros de los datos personales de quienes emiten dichas opiniones para poder identificarlos; así, deben solicitarse datos como nombre, correo electrónico, cédula de identidad o ciudadanía, además de implementar mecanismos para denunciar y eliminar los comentarios que lesionen los derechos garantizados en la constitución y la ley. De no cumplirse con lo anterior, los medios de comunicación serán responsables civil, penal y administrativamente por los comentarios.[62]

Restricción del anonimato

Existe una serie de reglas sobre registro o identificación, incluyendo la obligación de guardar registros de actividad en línea, que sin necesariamente prohibir o sancionar el anonimato, implican la formación de fuentes de información que comprometen la capacidad de comunicarse o expresarse de forma anónima. Dentro de tales reglas, encontramos las siguientes:

- Registro de teléfonos móviles de prepago: En varios países de América Latina existe este mandato legal, en otros se discute su implementación, como detalla Díaz (2017). Brasil comenzó a exigir el registro en 2003, mediante la Ley N.º 10.703 que dispone el registro de usuarios de teléfonos celulares prepagados.

  En Colombia, el registro de tarjetas SIM de todos los teléfonos móviles es obligatorio, justificando tal política pública para generar una lista tanto de los aparatos inscritos como una lista negra con los equipos robados.

  Ecuador comenzó a aplicar la obligación de registro a partir del año 2014, respecto de teléfonos móviles de prepago como de aquellos sujetos a pago mensual, con motivos similares a los del caso colombiano.

  Guatemala aprobó una ley de registro de teléfonos celulares el año 2013, con la cual se buscaba combatir el alza en los robos de estos dispositivos, además de establecer duras penas para tal delito.

  En Perú el proceso de identificación de los equipos de prepago comenzó el año 2010 con el Decreto Supremo 024-2010 MTC que aprueba el procedimiento para la subsanación de la información consignada en el registro de abonados prepago, y se justificó en el uso delictivo que puede darse a estas líneas anónimas.

  Chile no tiene ley sobre registro obligatorio de tarjetas SIM y equipos telefónicos de prepago, pero actualmente se están discutiendo en el Congreso Nacional dos proyectos de ley que buscan implementarlo.

  Como contrapunto a la realidad de todos los países latinoamericanos previamente enunciados está el caso de México, donde en 2009 comenzó a regir el registro obligatorio de tarjetas SIM. En agosto de 2011 se puso fin a dicha medida por varios motivos, entre ellos: no ayudó a disminuir la comisión de la clase de delitos que se buscaban combatir, sino que la tasa de aquellos aumentó; hubo muchos problemas en la práctica para implementar el registro de forma óptima, siendo las compañías de telecomunicaciones a menudo incapaces de comprobar si la información concedida por los clientes era real, además de pocos incentivos a los privados para procurar la calidad y veracidad de tales datos.[63]

---

62 ECUADOR, Asamblea Nacional. "Ley Orgánica de Comunicación". 25 de junio de 2013. En línea, disponible en http://www.cncine.gob.ec/imagesFTP/63228.5_LEY_ORGANICA_COMUNICACION.pdf [fecha de consulta:02 de noviembre de 2015]

63 GSMA. 2013. "The Mandatory Registration of Prepaid SIM Card Users". En línea, disponible en http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf [fecha de consulta: 04 de noviembre de 2015] p. 11.

Registros de tarjetas de identificación, transporte y datos biométricos: Existe una tendencia en Latinoamérica a recolectar una serie de datos de la población en los más diversos ámbitos y servicios. Gobiernos como el mexicano[64] y el peruano[65] han dictado leyes sobre geolocalización, permitiendo ambas ubicar los teléfonos que estén involucrados en actividad criminal, sin ser necesaria una orden judicial previa. A su vez, muchos estados han dispuesto o autorizado el uso de tecnologías biométricas para la verificación de identidad de las personas, en una tendencia creciente (Ferreyra y Ucciferri, 2017).

Si bien todos estos mecanismos no constituyen por sí solos restricciones al anonimato, representan una realidad que relativiza su efectividad: existen cada vez más puntos de información que, relacionados directamente con un nombre, o bien mediante la relación entre unos y otros, pueden ayudar a identificar a una persona.

CIFRADO

Respecto del cifrado de comunicaciones, hay pocas menciones en la normativa latinoamericana. Así solamente podemos hablar del caso colombiano, del caso brasileño y de la experiencia cubana, los únicos ordenamientos que han regulado su uso.

Brasil contempla a nivel constitucional una prohibición al anonimato, entendida como un límite al derecho a la libertad de expresión. Si bien dicha disposición no hace mención al uso de cifrado, en 2014 hubo dos casos que se analizaron a partir de tal prohibición, pero recayeron sobre la petición de sacar de circulación y proscribir el uso de software de comunicaciones cifradas: Cryptic y Secret.

Respecto al caso Secret,[66] el poder judicial brasileño solicitó tanto a Apple como a Google retirar la aplicación de sus plataformas de descarga. Secret consiste básicamente en una red social que permite chatear de forma anónima y que cifra los datos de los participantes, para así evitar que estos sean reconocidos. Cryptic,[67] por otro lado, es la versión de Secret para Windows Phone. Si bien los contenidos de los mensajes pueden ser vistos por todos, el cifrado era utilizado para resguardar la identidad de los usuarios de la misma, quienes vertían contenido sobre sus contactos de Facebook. La justicia brasileña no solo solicitó el retiro definitivo de dichas aplicaciones de las tiendas digitales de estas tres compañías, sino también pidió que, de alguna forma, se borrasen aquellas de los teléfonos que ya las tenían instaladas.[68]

El juez civil Paulo Cesar de Carvalho, quien conoció de la causa, señaló que: "La libertad de expresión no constituye un derecho absoluto, siendo numerosas las hipótesis en que su ejercicio entra en conflicto con otros derechos fundamentales o bienes jurídicos colectivos protegidos

---

64 FORBES STAFF. "¿De qué va la Ley de Geolocalización?". 16 de enero de 2014. Forbes México. En línea, disponible en http://www.forbes.com.mx/de-que-va-la-ley-de-geolocalizacion/ [fecha de consulta: 04 de noviembre de 2015]

65 PERÚ, Presidencia de la República. "Decreto Legislativo Nº 1182". 27 de julio de 2015. En línea, disponible en http://www.elperuano.com.pe/NormasElperuano/2015/07/27/1268121-1.html [fecha de consulta: 04 de noviembre de 2015]

66 BRITO, E. 2014. "Use o App Secret Para Descobrir Todos os Segredos de Seus Amigos". Techtudo. En línea, disponible en: http://www.techtudo.com.br/tudo-sobre/secret.html [fecha de consulta: 03 de febrero de 2016]

67 JESUS, A. 2014. "Com Cryptic, Compartilhe Seus Segredos Anonimamente no Windows Phone". Techtudo. En línea, disponible en: http://www.techtudo.com.br/tudo-sobre/cryptic-app.html [fecha de consulta: 03 de febrero de 2016]

68 SALA, M. 2014. Un Juez Brasileño Dicta que Google Elimine Secret de su Play Store y de los Smartphones de sus Usuarios. Hipertextual.com. En línea, disponible en: http://hipertextual.com/2014/08/eliminacion-secret-brasil [fecha de consulta: 04 de febrero de 2016]

constitucionalmente, las que serán resueltas mediante una ponderación de intereses en juego, a modo de garantizar el derecho a la honra, privacidad, igualdad y dignidad humana y, asimismo, proteger la infancia y adolescencia (...)",[69] resaltando así tanto la noción de uso del discurso anónimo como ámbito no protegido por el derecho a la libertad de expresión dentro del sistema legal de dicho país, como también indicando que la balanza se inclinó a favor de la protección de los derechos de los niños y adolescentes (dado que estas aplicaciones originalmente fueron cuestionadas porque su uso se vinculó a casos de bullying escolar), enfatizando en los usos ilegítimos del anonimato y cifrado.

Separadamente, la justicia brasileña ha ordenado en varias ocasiones el bloqueo de la operación del servicio WhatsApp en todo el país, en atención a la no entrega de copias de conversaciones privadas entre personas objeto de investigación. La compañía se negó a dicha entrega no por contumacia, sino por la imposibilidad de cumplimiento: las conversaciones de WhatsApp, incluso aquellas en sus servidores, están cifradas, y solamente se descifran en sus extremos. Pese a tal imposibilidad, el ataque judicial al cifrado se repitió en más de una ocasión.[70]

Colombia tiene una condición paradójica y dudosa. La Ley N.º 1.621 del año 2013, sobre inteligencia y contrainteligencia, establece en su artículo 44 parágrafo 2 que los operadores de servicios de telecomunicaciones deben ofrecer el servicio de llamadas de voz cifradas a personal del alto gobierno y de inteligencia. No obstante, para el resto de la población que utilicen equipos de comunicación que usen en el "espectro radioeléctrico", se encuentra prohibido el envío de mensajes "cifrados o en lenguaje ininteligible", según el artículo 102 de la Ley 418 de 1997. Esta prohibición ha sido renovada por múltiples leyes, de forma constante, y está vigente al menos hasta el año 2018 en su forma actual. Es dudoso, pero probable, que la prohibición alcance a la telefonía móvil (Castañeda, 2015) incluyendo desde el protocolo 3G de telefonía hasta las modernas aplicaciones cifradas de punto a punto.

Cuba contempla una mención normativa expresa sobre el uso del cifrado en la Resolución 179/2008 sobre Proveedores de Internet al Público, la cual fue modificada por la Resolución 102/2011 en el año 2011. En esta última versión del documento, en el artículo 19 se enumeran las obligaciones de dichos proveedores, estableciendo en la letra e de dicha disposición que "para la utilización de cualquier tipo de aplicación que implique el encriptamiento de la información a transmitir, es requisito tramitar la aprobación, de conformidad con lo establecido por las disposiciones vigentes que lo regulan". Así, es el Ministerio del Interior quien evaluará si concede o no tal autorización.

Esta norma ha sido criticada porque restringe de manera desproporcionada la libertad de expresión, privando a los usuarios del derecho a labrarse un espacio privado para la opinión y expresión sin fines ilegales.[71] Por otro lado, el solo hecho de solicitar autorización para usar cifrado enciende las alertas del Gobierno, sobre todo en caso que sea un miembro de grupos especialmente vulnerables quienes pidan tal permiso.

---

69 G1. "Justiça do ES Determina Remoção do Secret de Lojas de Aplicativos no Brasil". 20 de agosto de 2014. Globo.com. En línea, disponible en http://g1.globo.com/tecnologia/noticia/2014/08/justica-do-es-determina-remocao-do-secret-de-lojas-de-aplicativos-no-brasil.html [fecha de consulta: 02 de noviembre de 2015]

70 Sobre la cuarta vez, Correio, "Justiça do Rio de Janeiro manda bloquear WhatsApp", 19 de julio de 2016, disponible en: http://www.correio24horas.com.br/noticia/nid/justica-do-rio-de-janeiro-manda-bloquear-whatsapp/ [fecha de consulta: 12 de febrero de 2017]

71 CARTAYA, R. 2015. Critica Relator de ONU Control a Cifrado de Datos Personales en Cuba. Martínoticias.com. En línea, disponible en: http://www.martinoticias.com/content/cuba-internet-derechos-encriptacion/97366.html [fecha de consulta: 04 de febrero de 2015]

6.3. ANONIMATO Y CIFRADO EN LA LEGISLACIÓN CHILENA

Anonimato y reserva de identidad.

Ley de prensa

En Chile, de forma similar a la tendencia latinoamericana mayoritaria, no existe mención constitucional sobre el anonimato, sino que su primera manifestación de resguardo se puede encontrar en la legislación, en relación con las distintas formas de secreto profesional.

Relevante es lo relativo a los de medios de comunicación, en relación a fuentes periodísticas. La Ley Nº 19.733 sobre libertades de opinión e información y ejercicio del periodismo tiene menciones breves al respecto. El artículo 7º de esta ley, si bien no define el derecho a la reserva de fuente periodística, sí indica a quienes se extiende (y pueden hacerlo valer). Los directores, editores de medios de comunicación social, periodistas y alumnos de las escuelas de periodismo y los corresponsales extranjeros que ejerzan su actividad en Chile, tendrán derecho a mantener reserva sobre su fuente informativa, la que se extenderá a los elementos que obren en su poder y que permitan identificarla y no podrán ser obligados a revelar esta ni aun judicialmente.

La reserva de fuentes tiene límites. El artículo 1º de la ley de prensa chilena expresa que la libertad de emitir opinión y la de informar, sin censura previa, constituyen un derecho fundamental de todas las personas. Añade que el ejercicio de aquel incluye no ser perseguido ni discriminado a causa de las propias opiniones, buscar y recibir informaciones, y difundirlas por cualquier medio, sin perjuicio de responder de los delitos y abusos que se cometan, en conformidad a la ley. Reitera así lo ya señalado en la Constitución.

En virtud de lo anterior, la comisión de un hecho que revista el carácter de delito podría suponer la petición, previa orden judicial, de parte del ente persecutor para conocer los datos asociados a la fuente secreta. El Juez de Garantía eventualmente analiza en dicho contexto la proporcionalidad de la medida en tanto la lesión que puede causar en el derecho a la libertad de expresión en comparación a la magnitud del delito que se investiga, además de la idoneidad de la medida investigativa intrusiva.

Protección de datos personales. La ley Nº 19.628 sobre Protección de Datos Personales recoge los principios y derechos relativos al tratamiento de datos personales. Si bien no indica de forma expresa la posibilidad de aplicar mecanismos de anonimización, se contempla la autorización para que personas jurídicas privadas puedan tratar los datos de un titular sin su consentimiento. Esta es una situación excepcional y procede en aquellos para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.

Otra amplia autorización para el uso de datos personales existe a partir de la figura de la "fuente de acceso público", como origen de datos que permite su tratamiento de forma lícita y sin pedir consentimiento a sus titulares, como es el caso de bases de datos de acceso público. De este modo, dados los márgenes de desprotección, la recolección y tratamiento de datos en Chile permiten realizar los cruces suficientes para elaborar perfiles de personas, facilitando su identificación a partir de factores en principio disociados de identidad.

Por otra parte, la ley Nº 19.628 define al dato estadístico como el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable (Art. 2º literal e). Por tanto, si bien no es una mención expresa, la ley chilena permitiría tratar datos sin el consentimiento del titular o más allá del fin o período para el cual fueron recolectados, en tanto se haga de tal forma que no puedan vincularse al titular (Art. 4º inciso final). No existen disposiciones asociadas a la prevención o sanción de la desanonimización.

Investigación penal y retención de datos. Otra arista de la legislación nacional que entra en conflicto con el ejercicio del anonimato en línea consta en el marco legal sobre investigación y persecución criminal, además de las expresiones de este mismo contempladas en la regulación de telecomunicaciones.

El Código Procesal Penal, a partir del artículo 222, regula la medida intrusiva de interceptación de comunicaciones, incluidas las electrónicas. Este último punto crea una obligación que va en detrimento del anonimato: la retención de metadatos de telecomunicaciones. La ejecución de dicha medida se norma en mayor detalle en el Decreto 142 del Ministerio de Transporte y Telecomunicaciones (Subsecretaría de Telecomunicaciones de septiembre de 2005) también conocido como "Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de comunicaciones". La retención se extiende a los números IP desde los que se conectan equipos a internet, y el rango de números IP que mantiene cada proveedor de conexión. Con ello es posible, en teoría, aproximarse a quien comete un ilícito, al vincular una dirección a un rango de IP de una empresa de comunicaciones, que a su vez tendrá la información de los clientes con el uso de esos números IP.[72]

Sobre un intento mucho más rudimentario de registrar a quienes usan internet, el Tribunal Constitucional se pronunció el año 2011 al conocer preventivamente sobre un proyecto de ley que buscaba obligar a llevar registro de los usuarios de cibercafés. En tal oportunidad dicho tribunal dictaminó en el considerando vigésimo:

> **"Que, naturalmente, cualquiera entiende -aun sin ser jurisperito- que está a salvo en su legítima discreción para circular anónima e indistinguiblemente de los demás, sin chequeos o registros, a menos que a juicio de una autoridad competente hubiera causas probables que inciten a pensar que se están perpetrando ilícitos concretos y verosímiles. De suerte que, esto sentado, 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, hasta poder revelar las preferencias políticas, opciones comerciales e inclinaciones sociales de las personas;"**[73]

El Tribunal de Justicia de la Unión Europea en abril de 2014 declaró como inválida la Directiva sobre conservación de datos, levantando cuestionamientos similares a los señalados por el Tribunal Constitucional chileno tres años antes a propósito de los cibercafés. Expresó que tal medida viola el contenido esencial del derecho fundamental a la privacidad y a la protección de datos personales y que si bien hay un fin legítimo por el cual se produce tal afectación (seguridad pública), la lesión a tales derechos carece de proporcionalidad.[74] Queda en duda si habrá algún pronunciamiento similar en Chile a propósito de la persistente obligación de retención de datos de comunicación. El contraste es mayor cuando consideramos que en Europa se consideró como desproporcionado la conservación de al menos seis meses, siendo que en Chile es al menos de

---

72 Al respecto, para más detalles ver Díaz (2017).

73 CHILE, Tribunal Constitucional. 2011. Sentencia Rol N° 1894-2011-CPR (control preventivo de constitucionalidad), considerando vigésimo.

74 TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA. 2014. Comunicado de Prensa 54/14. En línea, disponible en: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf [fecha de consulta: 08 de febrero de 2016] pp. 1-2.

un año, sin un máximo. También debe considerarse que en el derecho de la Unión Europea se cuenta con una institucionalidad de protección de datos personales modelo para el resto del mundo, mientras que la ley chilena adolece de espacios de desprotección y de falta de adecuación a la realidad. Es más, Chile es de los pocos países de la región sin protección constitucional de datos personales (Remolina, 2012).

De este modo, la medida de interceptación y conservación de comunicaciones privadas, y su especial forma de puesta en marcha respecto de las comunicaciones realizadas a través de internet (con registros de IP) está en conflicto con la idea de permitir el anonimato en línea, en tanto otorga suficiente información para permitir elaborar perfiles precisos de los usuarios de tales servicios de telecomunicaciones, tema sobre el cual tanto dentro de Chile como a nivel europeo se ha llamado la atención por la afectación desproporcionada que produce a derechos fundamentales.

Registro de dispositivos móviles. En apoyo al combate al crimen de alta peligrosidad actualmente se tramitan tanto en la Cámara de Diputados como en el Senado un par de proyectos de ley que buscan introducir obligaciones de registro de tarjetas SIM de equipos móviles suscritos al régimen de prepago. Si bien ambas iniciativas están en trámite legislativo, contemplan disposiciones que descubren al anonimato en línea, haciendo plenamente identificable al sujeto detrás del teléfono. Además, considerando que en la actualidad el uso del internet móvil es más masivo que el de su vertiente fija, permitiría acumulaciones de información que van más allá de los datos personales del usuario y su número de teléfono.

Esto es incluso más crítico en el proyecto presentado por la cámara baja (Boletín 9767-15 del 09 de diciembre de 2014),[75] el cual establece a la SUBTEL como organismo a cargo de recibir la información de registro realizado en los puntos de venta de tales tarjetas, considerando que según la normativa de carácter procesal penal y administrativa anteriormente revisada, dicha subsecretaría ya cuenta con el registro de direcciones IP y de los sitios visitados por cada usuario, dotándola de mayores volúmenes de información que hacen ilusorio el anonimato en la red.

Anonimato en el espacio público:

En el considerando 23 de la sentencia rol STC 1984-2011 ya citada del Tribunal Constitucional chileno sobre el proyecto de ley que buscaba imponer el registro de usuarios de cibercafés, se resalta la importancia que tiene el espacio físico privado del individuo en relación al ejercicio de sus derechos y libertades fundamentales. En ese sentido, el Tribunal Constitucional manifestó:

> "VIGÉSIMOTERCERO: 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 (...).
>
> Así, no obstante que los cibercafés constituyen locales accesibles en general al público, en cuanto no se puede inadmitir a ningún cliente o usuario. A diferencia de otros lugares de afluencia masiva, suelen organizarse internamente en cámaras o cabinas individuales y reservadas, justamente en consideración a los servicios de interconexión que facilitan y a modo de cautelar que dentro de ellos tenga cobijo un cierto ámbito de privacidad. Igualmente internet, puesto que si bien esta red informática mundial

---

75 CHILE, Cámara de Diputados. 2014. Boletín N 9767-15 Exige a los Operadores de Telefonía Móvil Registrar los Datos Personales de los Clientes que Adquieran una Línea en la Modalidad de Prepago. En línea, disponible en: https://www.camara.cl/pley/pley_detalle.aspx?prmid=10187&prmboletin=9767-15 [fecha de consulta: 09 de febrero de 2016]

configura un espacio abierto, así como los correos electrónicos y la mensajería instantánea allí producidos, revisten carácter confidencial;".[76]

El fallo acá citado no solo reconoce que la privacidad en línea se manifiesta en el entorno digital, sino que también materialmente en un espacio físico. No solo basta otorgar reserva sobre la actividad del sujeto en la red y las cuentas de servicios de comunicaciones a través de internet que este pueda utilizar, sino que también respecto de la identidad física del sujeto, tal y como G. Marx postula. En efecto, el Tribunal Constitucional entiende que quien utiliza la red tiene una expectativa de privacidad que se extiende no solo a lo que realiza en internet sino también a que no se observe lo que está haciendo en el entorno digital por parte de otras personas. No solo debe resguardarse de mecanismos de identificación digital sino que también de aquellos aspectos que permitan entrometerse en su esfera privada, como lo es (en este caso) que otros observen la pantalla del equipo.

Más lejos en su expresión, pero sin impacto en sus alcances, resultó el fallo de la Corte de Apelaciones de Santiago de 21 de agosto de 2017, en causa Rol Nº 34.360-2017, resolviendo la acción constitucional de protección contra el uso de drones de videovigilancia en la comuna de Las Condes, en la Región Metropolitana de Santiago. Si bien vincula la posibilidad de circular anónimamente por espacios públicos, limita esa expectativa cuando se cometen ilícitos.

27º. En efecto, razonable es que al acceder a un lugar público cada persona aspire, entre otros aspectos, que sus conversaciones no sean de acceso público, como también que en su desplazamiento no sea objeto de registro personal o de seguimientos, es decir, que pueda deambular libremente manteniendo su anonimato frente a quienes le rodean, a menos que incurra en conductas ilegales o se vea involucrado en situaciones de emergencia, pues en tales casos, normal es que tales expectativas de privacidad se desvanezcan (…) [La grabación por parte de los drones] se trata además de vistas panorámicas de dichos lugares [públicos], que dejan a salvaguarda el anonimato de los transeúntes, a menos, claro está de situaciones delictivas o de emergencia en que el anonimato puede decrecer en pro de otros fines legítimos de seguridad.

El fallo culmina autorizando el uso de drones para la videovigilancia. No explica el vínculo entre una expectativa de ocultamiento de identidad como situación fáctica, de la expectativa normativa de mantener la identidad en reserva frente a una investigación de un agente estatal. Pero más allá de eso, discurre absurdamente sobre el registro audiovisual como un acto que no afectaría el anonimato, aun cuando es necesariamente un registro sobre el cuerpo de quienes vigila.

- Legislación sobre cifrado en Chile

  Sobre el cifrado de comunicaciones no existe regulación ni normativa aplicable alguna en Chile. Hasta el momento, tampoco han habido casos de relevancia en los cuales se haya señalado judicialmente que existe un derecho a poder ser utilizados libremente por la población, ni tampoco sobre prohibiciones establecidas por la jurisprudencia.

  Esto es particularmente importante a propósito de las posibilidades que entrega la ley chilena para incautar equipos informáticos, cuya información pueda estar cifrada, o para interceptar comunicaciones privadas cifradas entre sus extremos. No existen habilitaciones legales expresas en Chile para la adopción de medidas que permitan conocer el contenido de esos dispositivos o de esas comunicaciones cuando ellas están cifradas, ni para exigir claves de descifrado.

---

76 CHILE, Tribunal Constitucional. 2011. Sentencia Rol N° 1894-2011-CPR (control preventivo de constitucionalidad), considerando vigésimotercero.

Sin hacer referencia expresa sobre las herramientas de cifrado, el Código Procesal Penal contempla la posibilidad de realizar medidas investigativas intrusivas innominadas, tal y como dan cuenta los artículos 226 y el artículo 9º, el cual exige que de forma previa a la realización de una medida investigativa que "privare al imputado o aun tercero del ejercicio de los derechos que la Constitución asegura, o lo restringiere o perturbare", el Ministerio Público solicite y obtenga una autorización judicial.

De esta forma, teóricamente, podría pedirse al juez de garantía la orden para hackear un disco duro o el cifrado de una llave privada, aunque en la práctica sea altamente difícil o costoso de ejecutar, considerando la reciente experiencia global.

En efecto, la controversia entre Apple y el FBI en relación al iPhone de Syad Farook, uno de los responsables del ataque efectuado en diciembre de 2015 en Inland Regional Center, en San Bernardino, ha dejado en evidencia cómo un cifrado fuerte no puede ser hackeado siquiera por la misma compañía que lo implementó en su dispositivo. El problema se centró, principalmente, porque Farook configuró su teléfono para que luego de diez intentos fallidos de ingreso del código, se borrará toda la información contenida en el celular. De este modo, se limitaba el uso de un método de fuerza bruta.[77]

Para poder romper el cifrado, el FBI solicitó a Apple la elaboración de software que permitiese atravesar el código numérico del iPhone. La compañía se negó. Finalmente, el FBI pudo ingresar al dispositivo, contratando a un tercero anónimo externo que realizó el procedimiento.[78]

Latinoamérica difícilmente cuenta con las capacidades técnicas para poder acceder a un sistema protegido con cifrado. Por ello, la opción ajustada a derecho es la petición al titular de la cuenta de correo o dispositivo que él o ella misma den acceso al correo o documento específico que se quiera solicitar, siguiendo las reglas de la legislación procesal penal referida a medidas investigativas intrusivas. No tenemos certeza de que tal caso haya acontecido.

Dos sucesos recientes ponen en perspectiva la actitud del Estado chileno frente al cifrado.

En primer término, el valor de la criptografía está relevado en la Política Nacional de Ciberseguridad, oficialmente lanzada en abril de 2017. Conforme a la misma, con el fin de aumentar la seguridad y la confianza en el ciberespacio.

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.[79]

Adicionalmente, se destaca como ejemplo de desarrollo potencial de una industria local de ciberseguridad, el desarrollo a nivel local de estándares y uso de criptografía.

En segundo lugar, durante el mes de octubre de 2017, ocho miembros de comunidades mapuche al sur de Chile fueron detenidos, acusados de asociación ilícita terrorista, por diversos atentados contra la propiedad privada, en una zona de constante conflicto por las demandas de pueblos indígenas sobre territorios ancestrales, hoy mayormente bajo propiedad y explotación

---

77 DOMONOSKE, C y SELYUHK, A. 2016. Apple, The FBI And iPhone Encryption: A Look At What's At Stake. Npr.com. En línea, disponible en http://www.npr.org/sections/thetwo-way/2016/02/17/467096705/apple-the-fbi-and-iphone-encryption-a-look-at-whats-at-stake [fecha de consulta: 24 de abril de 2016]

78 Ibíd.

79 Política Nacional de Ciberseguridad, p. 19.

de empresas forestales. El Ministerio Público logró obtener la detención y la declaración de la medida de prisión preventiva para todos ellos, presentando entre sus antecedentes un informe de la Dirección de Inteligencia, Drogas e Investigación Criminal de Carabineros de Chile, que revelaba conversaciones entre los detenidos realizadas por WhatsApp.[80]

Ninguno de los antecedentes permitía suponer que Carabineros hubiera tenido acceso a los equipos móviles, ni que se hubiera infiltrado en las comunicaciones, pero el método técnico de obtención de la información estaba fuera de los antecedentes presentados por el Ministerio Público. La autorización judicial de intervención, se realizó dentro de las reglas de la Ley 19.974 sobre inteligencia del Estado, y en lugar de detallar el mecanismo se trataba de una autorización amplísima de interceptación de comunicaciones.

La Corte Suprema revocó la medida de prisión preventiva, pues la orden de tal medida carecía de justificación suficiente, al no expresar sus fundamentos ni sopesar en ello la argumentación de la defensa.[81] Los cuestionamientos ya se habían extendido, pues no habría habido suficiente asociación entre los apodos supuestamente usados en las conversaciones, los hechos dudosamente podían calificarse de terroristas, y porque en testimonio de la mujer de uno de los detenidos, él no usaba WhatsApp. Si efectivamente Carabineros cuenta con mecanismos para eludir el cifrado, o si simplemente se trataba de un montaje, es una duda que hoy persiste.

---

80 El Mercurio, "Mensajes entre mapuches detenidos dan cuenta de envío de armas desde Argentina", 26 de septiembre de 2017, página C2.

81 La Tercera, "Suprema ordena liberar a detenidos por Operación Huracán", 19 de octubre de 2017, http://www.latercera.com/noticia/suprema-ordena-liberar-detenidos-operacion-huracan/

7. CONCLUSIONES Y RECOMENDACIONES

El anonimato y el cifrado no son técnicas nuevas. Hoy en día se pueden lograr mediante el uso de herramientas informáticas, dado que parte fundamental de las amenazas y lesiones a los derechos a la libertad de expresión y resguardo de la vida privada se efectúan a través de la red. Así, son útiles para el ejercicio y respeto pleno de las libertades fundamentales, considerando que internet es hoy, el canal de preferencia para opinar e informarse.

Tanto Naciones Unidas como el sistema interamericano de derechos humanos, especialmente en los últimos tres años, han centrado su atención entre la relación entre internet y el efecto que tiene esta tecnología en los derechos humanos de la población. Han podido identificar su relevancia en el ejercicio, protección y promoción de tales derechos, pero también una serie de riesgos. Si bien algunos no son una novedad dentro de la historia de la humanidad, sí lo es su capacidad intrusiva, su alto alcance, intensidad de la afectación y, sobre todo, el bajo costo que representa para gobiernos y privados incurrir en dichas prácticas impunemente. Por lo mismo, para que el individuo pueda protegerse ante estos riesgos, se ha identificado al anonimato en línea y al uso de técnicas de cifrado como la forma más adecuada de proteger su privacidad y otros derechos.

Es por ello que estos mismos organismos, sobre todo Naciones Unidas, han enfatizado en que los gobiernos no deben prohibir que la población use tales mecanismos, sobre todo en caso de grupos identificados como especialmente vulnerables, incluyendo a las minorías étnicas y sociales, opositores políticos del gobierno de turno, miembros de la sociedad civil, defensores de derechos humanos e investigadores y académicos.

No obstante, los diferentes gobiernos del mundo han buscado regular aspectos de internet con miras a la protección de otros bienes jurídicos, especialmente la protección a la seguridad pública, muchas veces en detrimento de los derechos de la población. Para lo anterior, se establecen medidas que si bien cumplen con los requisitos de legalidad y necesidad, suelen no aprobar el test de proporcionalidad.

Los actuales modelos sobre regulación de internet suelen olvidar dos puntos claves: las características que diferencian a la red de otros servicios de telecomunicaciones y su importancia respecto al ejercicio de derechos humanos.

En América Latina, si bien es posible encontrar normativas y disposiciones que protegen el uso de anonimato y cifrado, también existen cuerpos legales y hasta menciones constitucionales que entorpecen su utilización, sumado a prácticas dentro de dichos Estados y de seguir la tendencia mundial a dar preeminencia a la persecución criminal por sobre la protección al sujeto.

Chile está en una situación intermedia en comparación a varios de sus países vecinos, pues presenta legislación anquilosada que produce ámbitos de desprotección. Además es apreciable una tendencia a presentar proyectos de ley que incluyen amenazas a la población que sí existen en otros países, o a seguir teniendo vigente o querer introducir medidas que en otras latitudes se han visto cuestionadas o de plano suprimidas del sistema legal.

Finalmente, existen todavía dudas de las respuestas del sistema normativo y del sistema persecutor cuando efectivamente existan razones que justifiquen eludir los mecanismos de ofuscación de identidad o de comunicaciones.

Por tanto, como propuestas de política pública podemos presentar:

- Abstenerse de establecer prohibiciones generalizadas o exigir el cumplimiento de requisitos que en la práctica funcionan como prohibición o restricción al uso de cifrado y anonimato en línea por parte de la población. Entre otros, abstenerse de leyes que

obliguen a la identificación para actos de expresión o comunicación, o que tengan por efecto la prohibición del anonimato o el cifrado.

- Abstenerse de perseguir a individuos y organizaciones que utilicen software de cifrado o el velo del anonimato en internet para manifestar de forma legítima su derecho a la libertad de expresión o busquen proteger su intimidad en línea.

- Abstenerse de elaborar normas legales o reglamentarias que impliquen restricciones a la circulación o distribución de tecnologías de cifrado de comunicaciones.

- Promover el uso generalizado de cifrado fuerte y anonimato en línea, especialmente en caso de grupos susceptibles de ser vigilados, como defensores de derechos humanos, activistas, investigadores, opositores políticos y minorías. De esta forma, se evita que quienes usen tales elementos sean especialmente distinguibles y, así también, monitoreados. La PNCS es un avance significativo en ese sentido.

- No solo abstenerse de exigir, sino prohibir la incorporación de vulnerabilidades intencionales a hardware y software para así acceder al contenido de comunicaciones y archivos cifrados, puesto que con ello se compromete la seguridad de la red entera.

- Abstenerse de exigir, legal o judicialmente, la entrega de una clave privada de cifrado, y abstenerse de establecer medidas de archivo de claves. Abstenerse también de solicitar la entrega de esta en el marco de una investigación criminal en busca de superar el cifrado que protege comunicaciones o archivos.

- Insistir, en el ejercicio de las potestades de persecución criminal y de enjuiciamiento de delitos, que se recurra a medidas de investigación y recolección de información de la forma menos intrusiva posible.

- Fortalecer la confianza y la sensación de seguridad, promoviendo iniciativas tales como prohibir el uso de vulnerabilidades informáticas introducidas intencionalmente. Esto no solo mejorará la percepción ciudadana sobre su privacidad y seguridad en línea, sino que también pondrá beneficia a privados (quienes no comprometen sus actividades y prestaciones de servicios en línea por estas vulnerabilidades en el sistema) y al mismo Estado ante el resto de la sociedad.[82]

- Establecer reglas claras para el uso de tecnologías altamente intrusivas en caso que sea justificado su uso, de modo tal que la descripción legal de la misma delimite la aplicación de la misma.

- Apuntar a cumplir los estándares de ciberseguridad globales, dando pronto curso a las medidas de la PNCS.

---

82 CASTRO, D y MCQUINN, A. 2016. Unlocking Encryption: Information Security and the Rule of Law. Information Technology & Innovation Foundation. En línea, disponible en: http://www2.itif.org/2016-unlocking-encryption.pdf [fecha de consulta: 31 de mayo de 2016] pp. 33-34

BIBLIOGRAFÍA:

ABELSON, H et al. 2015. Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications". Computer Science and Artificial Intelligence Laboratory Technical Report.

ACADEMIA DOMINICANA DE LA LENGUA. "*Encriptar". Academia Dominicana de la Lengua. En línea, disponible en http://academia.org.do/encriptar/ *[Fecha de consulta: 03 de diciembre de 2015]*

ARTHUR, C. 2013. How Internet Encryption Works. The Guardian. En línea, disponible en: http://www.theguardian.com/technology/2013/sep/05/how-internet-encryption-works *[Fecha de consulta: 10 de diciembre de 2015]*

BLUMENTHAL, M. 2007. "Encryption: Strengths and Weaknesses of Public-Key Cryptography". En línea, disponible en: http://www.csc.villanova.edu/~tway/courses/csc3990/f2007/csrs2007/01-pp1-7-MattBlumenthal.pdf *[Fecha de consulta: 07 de enero de 2016]*

BLUEPRINT FOR FREEDOM OF SPEECH. Peru – Whistleblowing Protection. blueprintforfreespeech.net. En línea, disponible en: https://blueprintforfreespeech.net/document/peru *[Fecha de consulta: 29 de abril de 2016]*

BOTERO, C. 2015. "En Defensa del Cifrado". ElEspectador.com. En línea, disponible en: http://www.elespectador.com/opinion/defensa-del-cifrado *[Fecha de consulta: 13 de enero de 2016]*

BRITO, E. 2014. "Use o App Secret Para Descobrir Todos os Segredos de Seus Amigos". Techtudo. En línea, disponible en: http://www.techtudo.com.br/tudo-sobre/secret.html *[Fecha de consulta: 03 de febrero de 2016]*

CARTAYA, R. 2015. Critica Relator de ONU Control a Cifrado de Datos Personales en Cuba. Martínoticias.com. En línea, disponible en: http://www.martinoticias.com/content/cuba-internet-derechos-encriptacion/97366.html *[Fecha de consulta: 04 de febrero de 2015]*

CASTAÑEDA, D. 2015. "La peligrosa ambigüedad de las normas sobre cifrado de comunicaciones en Colombia". Digital Rights LAC, disponible en: https://www.digitalrightslac.net/es/la-peligrosa-ambiguedad-de-las-normas-sobre-cifrado-de-comunicaciones-en-colombia/ *[Fecha de consulta: 27 de abril de 2016]*

CASTRO, D. 2011. Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising. The Information Technology & Innovation Foundation. En línea, disponible en: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/dae-library/benefits_and_limitations_of_industry_self-regulation_for_online_behavioral_advertising.pdf *[Fecha de consulta: 27 abril de 2016]*

CASTRO, D y MCQUINN, A. 2016. Unlocking Encryption: Information Security and the Rule of Law. Information Technology & Innovation Foundation. En línea, disponible en: http://www2.itif.org/2016-unlocking-encryption.pdf *[Fecha de consulta: 31 de mayo de 2016]*

CLEMENS, A. 2004. "No Computer Exception to the Constitution: The Fifth Amendment Protects Against Compelled Production of an Encrypted Document or Private Key" en UCLA Journal of Law and Technology 8(2). En línea, disponible en http://www.lawtechjournal.com/articles/2004/02_040413_clemens.pdf *[Fecha de consulta: 06 de enero de 2016]*

COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, Relatoría Especial Para la Libertad de Expresión. "Libertad de Expresión e Internet". 2013. COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, Relatoría Especial Para la Libertad de Expresión. "Libertad de Expresión e Internet".

CRYPTO MUSEUM. 2015. "Clipper Chip". Crypto Museum. En línea, disponible en http://www.cryptomuseum.com/crypto/usa/clipper.htm *[Fecha de consulta: 04 de enero de 2016]*

DECCAN HERALD. 2010. Internet Now Single Biggest Source of Global Information. Deccan Herald. En línea, disponible en: http://www.deccanherald.com/content/117379/internet-now-single-biggest-source.html *[Fecha de consulta: 09 de febrero de 2016]*

DIARIO HOY. "El Nuevo DNI de Randazzo en la Mira: Privacidad en Peligro". 30 de junio de 2014. Diario Hoy. En línea, disponible en http://diariohoy.net/politica/el-nuevo-dni-de-randazzo-en-la-mira-privacidad-en-peligro-30932 *[Fecha de consulta: 04 de noviembre de 2015]*

DÍAZ, Marianne. 2017. "Retención de datos y registro de teléfonos móviles: Chile en el contexto latinoamericano". En línea, disponible en https://www.derechosdigitales.org/wp-content/uploads/informe-marianne-retencion-de-datos.pdf *[Fecha de consulta: 23 de octubre de 2017]*

DIFFERENCEBETWEEN.NET. Difference Between PGP and GPG. Differencebetween.net. En línea, disponible en http://www.differencebetween.net/technology/software-technology/difference-between-pgp-and-gpg/ *[Fecha de consulta: 31 de mayo de 2016]*

DOMONOSKE, C y SELYUHK, A. 2016. Apple, The FBI And iPhone Encryption: A Look At What's At Stake. Npr.com. En línea, disponible en http://www.npr.org/sections/thetwo-way/2016/02/17/467096705/apple-the-fbi-and-iphone-encryption-a-look-at-whats-at-stake *[Fecha de consulta: 24 de abril de 2016]*

EL COMERCIO. 2015. WhatsApp es la App de Mensajería Más Popular del 2015. Elcomercio.pe. En línea, disponible en: http://elcomercio.pe/tecnologia/actualidad/whatsapp-app-mensajeria-mas-popular-2015-noticia-1862521 *[Fecha de consulta: 25 de abril de 2016]*

EL PAÍS. 2016. WhatsApp Activa el Cifrado de los Mensajes Para Todos los Usuarios. Elpaís.com. En línea, disponible en: http://tecnologia.elpais.com/tecnologia/2016/04/05/actualidad/1459875233_301649.html *[Fecha de consulta: 25 de abril de 2016]*

EWOW. 2014. "Educación y Ciencia, Cifrado Asimétrico" citado en VILLALOBOS, J. 2014. "Consideraciones para el uso de Cifrado en las Bases de Datos". 31 de julio de 2014. .Seguridad. En línea, disponible en http://revista.seguridad.unam.mx/numero22/consideraciones-para-el-uso-de-cifrado-en-las-bases-de-datos *[Fecha de consulta: 03 de diciembre de 2015]*

FARIVAR, C. 2015. Paris Police Find Phone With Unencrypted SMS Saying "Let's go, We're Starting". Armstechnica.com. En línea, disponible en: http://arstechnica.com/tech-policy/2015/11/paris-police-find-phone-with-unencrypted-sms-saying-lets-go-were-starting/ *[Fecha de consulta: 25 de abril de 2016]*

FERREYRA, E. y UCCIFERRI, L. 2017. Cuantificando identidades en América Latina. https://adcdigital.org.ar/wp-content/uploads/2017/06/ADC-Cuantificando-identidades-en-LatAm.pdf *[Fecha de consulta: 20 de octubre de 2017]*

FORBES STAFF. "¿De qué va la Ley de Geolocalización?". 16 de enero de 2014. Forbes México. En línea, disponible en: http://www.forbes.com.mx/de-que-va-la-ley-de-geolocalizacion/ *[Fecha de consulta: 04 de noviembre de 2015]*

FUNDÉU BBVA. "Encriptar es Oculta un Mensaje con una Clave". Fundéu BBVA. En línea, disponible en http://www.fundeu.es/recomendacion/encriptar-es-un-termino-valido/ *[Fecha de consulta: 03 de diciembre de 2015]*

G1. "Justiça do ES Determina Remoção do Secret de Lojas de Aplicativos no Brasil". 20 de agosto de 2014. Globo.com. En línea, disponible en http://g1.globo.com/tecnologia/noticia/2014/08/justica-do-es-determina-remocao-do-secret-de-lojas-de-aplicativos-no-brasil.html *[Fecha de consulta: 02 de noviembre de 2015]*

GARCÍA, L. 2004. La Protección de la Identidad de las Fuentes Periodísticas a la Luz de los Instrumentos Internacionales de Derechos Humanos y de los Estándares de sus Órganos de Aplicación. Anuario de Derecho Constitucional. En línea, disponible en: http://www.juridicas.unam.mx/publica/librev/rev/dconstla/cont/2004.2/pr/pr10.pdf *[Fecha de consulta: 29 de enero de 2016]*

GELLMAN, B y NAKASHIMA, E. 2015. "As Encryption Spreads, U.S. Grapples with Clash Between Privacy, Security". The Washington Post. En línea, disponible en https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html *[Fecha de consulta: 06 de enero de 2016]*

GILBERTSON, S. 2010. "Why Your Digital Fingerprint Makes You Easy to Track". Wired.co.uk. En línea, disponible en: http://www.wired.co.uk/news/archive/2010-01/29/your-digital-fingerprint-makes-you-easy-to-track *[Fecha de consulta: 19 de enero de 2016]*

GONZÁLEZ, G. 2014. "Cómo Crear una Contraseña Súper Segura en Cinco Sencillos Pasos". Hipertextual.com. En línea, disponible en http://hipertextual.com/archivo/2014/06/crear-contrasena-segura/ *[Fecha de consulta: 07 de enero de 2016]*

GRABOW, R. 1997. McIntyre v. Ohio Elections Commission: Protecting the Freedom of Speech or Damaging the Electoral Process?. Catholic University Law Review 46(2). En línea, disponible en: http://scholarship.law.edu/cgi/viewcontent.cgi?article=1542&context=lawreview *[Fecha de consulta: 05 de mayo de 2016]*

GREENBERG, A. 2014. "Hacker Lexicon: What is End-to-End Encryption?". Wired.com. En línea, disponible en: http://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/ *[Fecha de consulta: 18 de enero de 2016]*

GREENE, T. 2015. "Mandating Backdoors for Encrypted Communications is a Bad Idea". Networkworld. En línea, disponible en: http://www.networkworld.com/article/2945374/security0/mandating-backdoors-for-encrypted-communications-is-a-bad-idea.html *[Fecha de consulta: 12 de enero de 2016]*

GSMA. 2013. The Mandatory Registration of Prepaid SIM Card Users: A White Paper. En línea, disponible en: http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf *[Fecha de consulta: 09 de febrero de 2016]*

GSMA. 2014. The Mobile Econonomy Latin America 2014. En línea, disponible en: http://www.gsmamobileeconomylatinamerica.com/GSMA_Mobile_Economy_LatinAmerica_2014.pdf *[Fecha de consulta: 09 de febrero de 2016]*

HENN, S y SELYUKH, A. 2015. "After Paris Attacks, Encrypted Communication Is Back In Spotlight". NPR.org. En línea, disponible en http://www.npr.org/sections/alltechconsidered/2015/11/16/456219061/after-paris-attacks-encrypted-communication-is-back-in-spotlight *[Fecha de consulta: 05 de enero de 2016]*

HERNÁNDEZ, V. (2016). Libertad de Expresión y Anonimato. En: ASOCIACIÓN POR LOS DERECHOS CIVILES. Libertad de Expresión en el Ámbito Digital. El Estado de la Situación en Latinoamérica, pp. 7-45.

HIGGINS, P. 2015. On the Clipper Chip's Birthday, Looking Back on Decades of Key Escrow Failures. Eff.org. En línea, disponible en: https://www.eff.org/deeplinks/2015/04/clipper-chips-birthday-looking-back-22-years-key-escrow-failures *[Fecha de consulta: 25 de abril de 2016]*

HIRSCH, D. 2011. The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?. Seattle University Law Review 34. En línea, disponible en: http://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=2003&context=sulr *[Fecha de consulta: 01 de febrero de 2016]*

HOW-TO-GEEK. "Brute-Force Attacks Explained: How All Encryption is Vulnerable". How-to-Geek.com. En línea, disponible en: http://www.howtogeek.com/166832/brute-force-attacks-explained-how-all-encryption-is-vulnerable/ *[Fecha de consulta: 07 de enero de 2016]*

INGRAHAM, N. 2013. 'Harry Potter' Author J.K. Rowling Assumed Male Identity to Secretly Release a Detective Novel. The Verge. En línea, dsponible en: http://www.theverge.com/2013/7/14/4522398/harry-potter-author-j-k-rowling-secretly-releases-detective-novel *[Fecha de consulta: 29 de enero de 2016]*

JESUS, A. 2014. "Com Cryptic, Compartilhe Seus Segredos Anonimamente no Windows Phone". Techtudo. En línea, disponible en: http://www.techtudo.com.br/tudo-sobre/cryptic-app.html *[Fecha de consulta: 03 de febrero de 2016]*

JUST, M. 2011. Key Escrow Definition en JAJODIAL, S y VAN TILBORG, H (editores) 2011. "Encyclopedia of Cryptography and Security". Estados Unidos, Springer USA, segunda edición.

KOEBLER, J. 2014. "How the NSA (Or Anyone Else) Can Crack Tor's Anonymity". Motherboard. En línea, disponible en:http://motherboard.vice.com/read/how-the-nsa-or-anyone-else-can-crack-tors-anonymity *[Fecha de consulta: 19 de enero de 2016]*

LEE, M. 2015. Microsoft Gives Details About its Controversial Disk Encryption. The Intercept. En línea, disponible en https://theintercept.com/2015/06/04/microsoft-disk-encryption/ *[Fecha de consulta: 11 de diciembre de 2015]*

LEONARD, J. 2015. "US to Take Backdoor Approach to Introducing Backdoors to Counter Encryption". Computing.uk. En línea, disponible en http://www.computing.co.uk/ctg/news/2426334/us-to-take-backdoor-approach-to-introducing-backdoors-to-counter-encryption *[Fecha de consulta: 05 de enero de 2016]*

LEVY, S. 1994. "Battle of the Clipper Chip". The New York Times. En línea, disponible en http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?module=-Search&mabReward=relbias:r,{%221=%22:=%22RI:6=%22}=&src=pm&pagewanted=2&_r=0 *[Fecha de consulta: 15 de diciembre de 2015]*

LIN, F. 2010. "Cryptography's Past, Present, and Future Role in Society". En línea, disponible en https://engineering.wustl.edu/current-students/student-services/ecc/Documents/Lin.pdf *[Fecha de consulta: 06 de enero de 2016]*

MARX, G. 2001. "Identity and Anonymity: Some Conceptual Distinctions and Issues for Research" en Documenting Individual Identity: The Development of State Practices in the Modern World. Princeton University Press. En línea, disponible en http://web.mit.edu/gtmarx/www/identity.html *[Fecha de consulta: 19 de octubre de 2015]*

McCULLOUGH, B. 2014. "The NSA Tried this Before -What the 90s Debate Over the Clipper Chip can Teach Us About Digital Privacy". Internet History Podcast. En línea, disponible en http://www.internethistorypodcast.com/2014/08/the-nsa-tried-this-before-what-the-90s-debate-over-the-clipper-chip-can-teach-us-about-digital-privacy-debates/ *[Fecha de consulta: 04 de enero de 2016]*

MEO, A. 2010. Consentimiento Informado, Anonimato y Confidencialidad en Investigación Social. La Experiencia Internacional y el Caso de la Sociología en Argentina. Aposta. Revista de Ciencias Sociales. En línea, disponible en: http://apostadigital.com/revistav3/hemeroteca/aines.pdf *[Fecha de consulta: 05 de mayo de 2016]*

McDONALD, W. Søren Kierkegaard (1813—1855). Internet Encyclopedia of Philosophy. En línea, disponible en: http://www.iep.utm.edu/kierkega/ *[Fecha de consulta: 29 de enero de 2016]*

MINISTERIO DE SEGURIDAD, "La Presidenta Presentó el SIBIOS". 07 de noviembre de 2011. Ministerio de Seguridad. En línea, disponible en http://www.minseg.gob.ar/la-presidenta-present%C3%B3-el-sibios *[Fecha de consulta: 04 de noviembre de 2015]*

MINISTERIO DE TRANSPORTE Y TELECOMUNICACIONES, Subsecretaría de Telecomunicaciones. 2014. Sector Telecomunicaciones. En línea, disponible en: http://www.subtel.gob.cl/wp-content/uploads/2015/01/PPT-Series-Septiembre-2014-041214-v1.pdf *[Fecha de consulta: 09 de febrero de 2016]*

MOYA, R. 2003. La Libertad de Expresión en la Red Internet. Revista Chilena de Derecho Informático 2.

NPR STAFF. 2015. Apple CEO Tim Cook: 'Privacy Is A Fundamental Human Right'. NPR.org. En línea, disponible en: http://www.npr.org/sections/alltechconsidered/2015/10/01/445026470/apple-ceo-tim-cook-privacy-is-a-fundamental-human-right *[Fecha de consulta: 11 de enero de 2016]*

PC MAGAZINE ENCYCLOPEDIA. "Definition of Back Door". PC Magazine.com. En línea, disponible en http://www.pcmag.com/encyclopedia/term/38339/back-door *[Fecha de consulta: 05 de enero de 2016]*

PEREZ, E y PROKUPECZ, S. 2015. "First on CNN: Paris Attackers Likely Used Encrypted Apps, Officials Say". CNN. En línea, disponible en http://edition.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/ *[Fecha de consulta: 05 de enero de 2015]*

PRIVACY INTERNATIONAL. 2015. Securing Safe Spaces Online: Encryption, Online Anonymity and Human Rights. En línea, disponible en: https://www.privacyinternational.org/sites/default/files/Securing%20Safe%20Spaces%20Online_0.pdf *[Fecha de consulta: 29 de enero de 2016]*

PRIVACY INTERNATIONAL. What is Metadata?. Privacyinternanal.org. En línea, disponible en: https://www.privacyinternational.org/node/53 *[Fecha de consulta: 11 de enero de 2016]*

REMOLINA, N. 2012. Aproximación Constitucional de la Protección de Datos Personales en Latinoamérica. Revista Internacional de Protección de Datos Personales 1.

ROGAWAY, P. 2015. The Moral Character of Cryptographic Work". En línea, disponible en: http://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf *[Fecha de consulta: 10 de diciembre de 2015]*

SALA, M. 2014. Un Juez Brasileño Dicta que Google Elimine Secret de su Play Store y de los Smartphones de sus Usuarios. Hipertextual.com. En línea, disponible en: http://hipertextual.com/2014/08/eliminacion-secret-brasil *[Fecha de consulta: 04 de febrero de 2016]*

SANS INSTITUTE. 2001. "History of Encryption". En línea, diponible en https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730 *[Fecha de consulta: 03 de diciembre de 2015]*

SHAIK, R. 2014. How Crucial is Anonymity for Sexual Exploration and Promoting Sexual Rights Activism. Genderit.org. En línea, disponible en: http://www.genderit.org/es/node/4147 *[Fecha de consulta: 29 de enero de 2016]*

SIMPSON, D. 2015. Letter to the Editor: The Benefits of Anonymous Political Speech. The Washington Post. En línea, disponible en: https://www.washingtonpost.com/opinions/the-benefits-of-anonymous-political-speech/2015/01/25/092abefe-a326-11e4-91fc-7dff95a14458_story.html *[Fecha de consulta: 29 de enero de 2016]*

SOLOVE, D, ROTENBERG, M and SCHWARTZ, P. 2006. Privacy, Information and Technology. New York, ASPEN Publishers.

TEMPLE-RASTON, D. 2015. "FBI Director Says Agents Need Access To Encrypted Data To Preserve Public Safety". NPR.org. En línea, disponible en http://www.npr.org/sections/the-two-way/2015/07/08/421251662/fbi-director-says-agents-need-access-to-encrypted-data-to-preserve-public-safety *[Fecha de consulta: 05 de enero de 2016]*

THE GUARDIAN. 2008. Harmful Content on the Internet: Self-Regulation is the Best Way Forward. The Guardian. En línea, disponible en: http://www.theguardian.com/media/organ-grinder/2008/aug/01/post88 *[Fecha de consulta: 01 de febrero de 2016]*

USLegal. "Data Encryption Law & Legal Definition". uslegal.com. En línea, disponible en http://definitions.uslegal.com/d/data-encryption/ *[Fecha de consulta: 03 de diciembre de 2015]*

USLegal. "Malware Law & Legal Definition". uslegal.com. En línea, disponible en: http://definitions.uslegal.com/m/malware/ *[Fecha de consulta: 07 de enero de 2016*]

VÉLIZ, C. 2013. 'Whistleblowers': Los Canarios Morales en la Mina de la Democracia. The Huffington Post. En línea, disponible en: http://www.huffingtonpost.es/carissa-veliz/whistleblowers-los-canari_b_3560252.html *[Fecha de consulta: 29 de enero de 2016]*

VOCABULARY.COM., "Anonymity". En línea, disponible en: http://www.vocabulary.com/dictionary/anonymity *[Fecha de consulta: 15 de octubre de 2015]*

VOORHOOF, D. 2010. "Internet and the Right of Anonymity" en Proceedings of the Conference Regulating the Internet. Belgrado, 2010.

WYSOPAL, C. "Static Detection of Application Backdoors". En línea, disponible en http://www.veracode.com/sites/default/files/Resources/Whitepapers/static-detection-of-backdoors-1.0.pdf *[Fecha de consulta: 06 de enero de 2016]*

ZAMORANO, E. 2012. Chile: Servel Publicó Datos de 13 Millones de Ciudadanos. FayerWayer. En línea, disponible en: https://www.fayerwayer.com/2012/08/chile-servel-publico-datos-personales-de-13-millones-de-ciudadanos/ *[Fecha de consulta: 04 de febrero de 2016]*

ZETTER, K. 2015. "Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors". Wired.com. En línea, disponible en: http://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/ *[Fecha de consulta: 12 de enero de 2016]*

ZIMMERMANN, P. 1999. Why I Wrote PGP: Part of the Original 1991 PGP's User Guide (updated in 1999). philzimmermann.com. En línea, disponible en https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html *[Fecha de consulta: 09 de diciembre de 2015]*

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES:

ARGENTINA, Cámara de Diputados de la Nación. 2008. "Ley Nº 25.326 Sobre Protección de Datos Personales Y Normas Reglamentarias y Complementarias". En línea, disponible en http://www1.hcdn.gov.ar/dependencias/dip/textos%20actualizados/25326.010408.pdf *[Fecha de consulta: 05 de noviembre de 2015]*

BRASIL, Lei nº 10.703, de 18 de julho de 2003. En línea, disponible en http://www.anatel.gov.br/legislacao/leis/469-lei-10703 *[Fecha de consulta: 04 de noviembre de 2015]*

BRASIL, Cámara de Diputados. "Constitución Federal de la República de Brasil". 2010. En línea, disponible en http://english.tse.jus.br/arquivos/federal-constitution *[Fecha de consulta: 04 de noviembre de 2015]*

CHILE, Cámara de Diputados. 2014. Boletín N 9767-15 Exige a los Operadores de Telefonía Móvil Registrar los Datos Personales de los Clientes que Adquieran una Línea en la Modalidad de Prepago. En línea, disponible en: https://www.camara.cl/pley/pley_detalle.aspx?prmid=10187&prmboletin=9767-15 *[Fecha de consulta: 09 de febrero de 2016]*

CHILE. 2000. Código Procesal Penal. En línea, disponible en: http://www.leychile.cl/Navegar?idNorma=176595 [*Fecha de consulta: 08 de febrero de 2016]*

CHILE, Ministerio Secretaría General de Gobierno. 2001. "Ley Nº 19.733 Sobre Libertades de Opinión e Información y Ejercicio del Periodismo". En línea, disponible en http://www.leychile.cl/Navegar?idNorma=186049 *[Fecha de consulta: 04 de febrero de 2016]*

CHILE, Ministerio de Transporte y Telecomunicaciones, Subsecretaría de Telecomunicaciones. 2005. Decreto 142 del Ministerio de Transporte y Telecomunicaciones, Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de comunicaciones. En línea, disponible en: http://www.leychile.cl/Navegar?idNorma=242261 *[Fecha de consulta: 08 de febrero de 2016]*

CHILE, Tribunal Constitucional. 2011. Sentencia Rol N° 1894-2011-CPR (control preventivo de constitucionalidad).

COLOMBIA. Corte Constitucional. 2009. Sentencia T-298/09 Deberes Constitucionales de los Medios de Comunicación. corteconstitucional.gov.co. En línea, disponible en: http://www.corteconstitucional.gov.co/relatoria/2009/T-298-09.htm *[Fecha de consulta: 02 de mayo de 2016]*

COLOMBIA, Ministerio de Defensa Nacional. 2009. "Resolución 912 de 2008". En línea, disponible en https://www.redjurista.com/documents/r_mdef_0912_2008.aspx *[Fecha de consulta: 03 de noviembre de 2015]*

CORTE INTERAMERICANA DE DERECHOS HUMANOS, Caso Escher y Otros v Brasil (Sentencia de 06 de julio de 2009). En línea, disponible en http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf *[Fecha de consulta: 19 de octubre de 2015]*

CUBA, Ministerio de la Informática y las Comunicaciones. 2011. "Resolución 102/2011". En línea, disponible en: http://www.di.sld.cu/documentos/resol/resol_102_2011.pdf *[Fecha de consulta: 04 de febrero de 2015]*

ECUADOR, Asamblea Nacional. "Ley Orgánica de Comunicación". 25 de junio de 2013. En línea, disponible en http://www.cncine.gob.ec/imagesFTP/63228.5_LEY_ORGANICA_COMUNICACION.pdf *[Fecha de consulta: 02 de noviembre de 2015]*

ECUADOR, Arcotel. 2013. "Codificación de la Norma que Regula el Procedimiento para el Empadronamiento de Abonados del Servicio Móvil Avanzado (SMA) y Registro de Terminales Perdidos, Robados o Hurtados". En línea, disponible en http://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/07/codificacion_norma_empadronamiento.pdf *[Fecha de consulta: 03 de noviembre de 2015]*

ECUADOR. 2008. "Constitución de la República del Ecuador". En línea, disponible en: http://www.oas.org/juridico/PDFs/mesicic4_ecu_const.pdf *[Fecha de consulta: 02 de febrero de 2016]*

GUATEMALA, 2013. "Decreto Número 8-2013. Ley de Equipos Terminales Móviles". En línea, disponible en: http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs%20leyes/2013/pdfs/decretos/D08-2013.pdf *[Fecha de consulta: 03 de noviembre de 2015]*

KONRAD-ADENAUER-STITFUNG. "Cláusulas de Libertad de Expresión: Venezula". En línea, disponible en http://www.kas.de/upload/auslandshomepages/medioslatinos/venezuela/clausulas_de_libertad_de_expresion_-_venezuela.pdf *[Fecha de consulta: 02 de noviembre de 2015]*

KONRAD-ADENAUER-STITFUNG. "Constitución de la Nación Argentina". En línea, disponible en http://www.kas.de/upload/auslandshomepages/medioslatinos/argentina/argentina_constitucion.pdf *[Fecha de consulta: 04 de noviembre de 2015]*

NACIONES UNIDAS, Consejo de Derechos Humanos. 2011. "Informe del Representante Especial del Secretario General para la Cuestión de los Derechos Humanos y las Empresas Transnacionales y Otras Empresas, John Ruggie". En línea, disponible en: http://www.ohchr.org/Documents/Issues/Business/A.HRC.14.27_sp.pdf *[Fecha de consulta: 13 de enero de 2016]*

NACIONES UNIDAS, ORGANIZACIÓN ESTADOS AMERICANOS. 2013. Declaración Conjunta Sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión. En línea, disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927 *[Fecha de consulta: 29 de enero 2016]*

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Comisión Interamericana de Derechos Humanos. Declaración Sobre Principios Sobre Libertad de Expresión. En línea, disponible en: https://www.cidh.oas.org/basicos/basicos13.htm *[Fecha de consulta: 02 de mayo de 2016]*

ORGANIZACIÓN DE ESTADOS AMERICANOS. Comisión Interamericana de Derechos Humanos. 2015. Informe Anual de la Comisión Interamericana de Derechos Humanos 2014. Informe Anual de la Relatoría Especial para la Libertad de Expresión. En línea, disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/anuales/Informe%20Anual%202014.pdf *[Fecha de consulta: 28 de enero de 2016]*

PANAMÁ, Asamblea Nacional Legispam. 2005."Ley Número 22 de 2005 Que Prohíbela Imposición de Sanciones por Desacato, Dicta Medidas en Relación al Derecho a Réplica,

Rectificación o Respuesta y Adopta Otras Disposiciones". En línea, disponible en http://www.oas.org/juridico/spanish/mesicic2_pan_anexo_34_sp.pdf *[Fecha de consulta: 05 de noviembre de 2015]*

PARAGUAY, Convención Nacional Constituyente. "Constitución Nacional". 1992. En línea, disponible en http://www.oas.org/juridico/spanish/par_res3.htm *[Fecha de consulta: 04 de noviembre de 2015]*

PERÚ, Congreso de la República. 2013. "Ley Nº 29.733 de Protección de Datos Personales". En línea, disponible en http://www.claro.com.pe/portal/recursos/pe/pdf/Ley29733.pdf *[Fecha de consulta: 05 de noviembre de 2015]*

PERÚ, Presidencia de la República. 2015. "Decreto Legislativo Nº 1182". 27 de julio de 2015. En línea, disponible en http://www.elperuano.com.pe/NormasElperuano/2015/07/27/1268121-1.html *[Fecha de consulta: 04 de noviembre de 2015]*

PERÚ, Presidencia de la República. 2010. "Decreto Supremo Nº 024-2010-MTC que Aprueba el Procedimiento para la Subsanación de la Información Consignada en el Registro de Abonados Pre Pago". En línea, disponible en transparencia.mtc.gob.pe/idm_docs/normas_legales/1_0_1902.pdf *[Fecha de consulta: 04 de noviembre de 2015]*

REPÚBLICA BOLIVARIANA DE VENEZUELA, Asamblea Nacional. 2004. "Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos". En línea, disponible en http://www.nci.tv/archivos/Ley-de-Responsabilidad-Social-en-Radio-Television-y-Medios-Electr%C3%B3nicos.pdf *[Fecha de consulta: 03 de noviembre de 2015]*

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA. 2014. Comunicado de Prensa 54/14. En línea, disponible en: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf *[Fecha de consulta: 08 de febrero de 2016]*

UNITED NATIONS. 2012. General Assembly, Human Rights Council. Twentieth Session. Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development. En línea, disponible en: ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc *[Fecha de consulta: 25 de abril de 2015]*

UNITED NATIONS, Human Rights Council. 2015. "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of opinion and Expression, David Kaye".

UNITED NATIONS. 2014. The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights. En línea, disponible en: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf *[Fecha de consulta: 09 de febrero de 2016]*

URUGUAY, Comunicaciones e Informaciones. 2002. "Ley Nº 16.099 Díctanse Normas Referentes a Expresión, Opinión y Difusión, Consagradas por la Constitución de la República". En línea, disponible en http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=16099&Anchor= *[Fecha de consulta: 05 de noviembre de 2015]*


DERECHOS
DIGITALES
América Latina