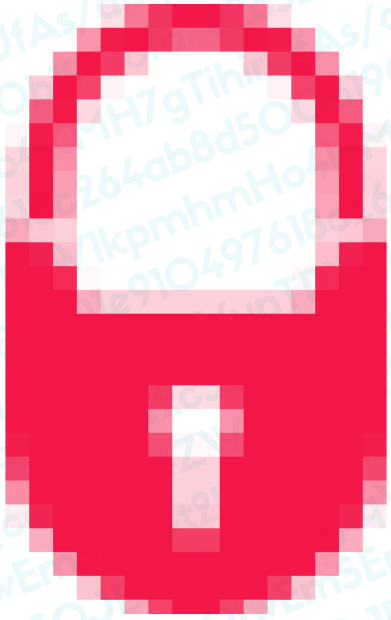
DEFENDIENDO LOS DERECHOS HUMANOS EN LA ERA DIGITAL



El rol del cifrado

por los Derechos Civiles

Área de Privacidad

con el apoyo de

PRIVACY INTERNATIONAL

Diciembre 2016

https://adcdigital.org.ar

Defendiendo los derechos humanos en la era digital: El rol del cifrado*

I Introducción

Hoy en día, más de tres mil millones de personas en todo el mundo tienen acceso a Internet. En Argentina, según un estudio de la UIT, la penetración de internet aumentó a un 69% hacia fines del 2015, en relación al 65% de 2014; el 80% de la población, unas 33 millones de personas, son usuarios activos de internet.[1]

El Estado, las agencias y dependencias gubernamentales, las empresas, los hospitales, almacenan nuestra información en bases de datos y computadoras conectadas a internet. Los dispositivos que utilizamos todos los días como nuestros smartphones (celulares inteligentes) y computadoras, a los cuales se suman otro sin fin de objetos conectados a internet en el mundo conocido como internet de las cosas (o Internet of Things): automóviles, relojes, televisores, tostadoras, lavarropas, hornos. Todos estos dispositivos almacenan y transmiten constantemente información personal a medida que vamos incorporándolos como parte de nuestra rutina y actividades cotidianas.

Este constante uso de dispositivos genera un inmenso flujo de datos, en forma de emails y mensajes, fotografías, notas, listas de pendientes, sitios web que visitamos, información de nuestras tarjetas de crédito y actividad bancaria, registros de salud, a la vez que también reflejan nuestros gustos musicales y de entretenimiento, creencias y orientación política, por mencionar tan solo algunos. A medida que vamos involucrando cada vez más en nuestras vidas a nuestros smartphones, computadoras, tablets, estos –gracias a la información y datos allí almacenados– se van convirtiendo en una representación digital de nuestra personalidad, de nuestra identidad como individuos. Así, los dispositivos se vuelven una extensión de nuestra mente.

---

*El presente informe fue producido por Leandro Ucciferri, abogado e investigador de las Áreas de Privacidad y Libertad de Expresión de la Asociación por los Derechos Civiles.

[1] Freedom On the Net, Freedom House, 2016, p.3. Disponible en (PDF): https://freedomhouse.org/sites/default/files/FOTN%202016%20Argentina.pdf

La creciente generación de información y datos no podría venir sin los característicos riesgos que este tipo de actividades implica. Lo que es preciado para unos, es deseado por otros. Nuestra información personal está en constante peligro de ser objeto de robo y espionaje, sea por criminales, atacando directamente individuos para extorsionar en busca de dinero, o yendo contra la fuente principal como son los servidores de las empresas que hospedan los datos, así como también por algunos gobiernos y determinadas empresas del sector privado que espían a los ciudadanos y usuarios.[2]

Frente a este panorama, el cifrado es una herramienta esencial que nos permite proteger desde nuestra información, hasta nuestra integridad física, a la vez que resguarda y ayuda a potenciar el goce y ejercicio de derechos humanos.

II ¿Qué es el cifrado?

Es el proceso a través del cual, mediante algoritmos matemáticos, se codifica el contenido de cualquier información -mensajes, fotografías, llamadas, videos- asegurándolo para que el mismo tan solo pueda ser accesible por su dueño o los destinatarios específicos que determine la persona que cifró la información.

Por otra parte, la criptografía "es la disciplina que engloba los principios, medios y métodos para la transformación de los datos con el fin de ocultar la información que contengan, establecer su autenticidad, prevenir alteraciones no detectadas, y prevenir su uso no autorizado".[3]

Si bien, como ocurre generalmente en las disciplinas vinculadas con la tecnología, hay una inmensa cantidad de herramientas y protocolos que implementan el cifrado de diversas maneras, podemos mencionar tres tipos de cifrado que las personas encuentran en su día a día, aún sin pertenecer a comunidades que trabajen sobre la temática.

Cifrado de disco completo o de dispositivo (o *full-disk encryption*): es el proceso a través del cual toda la información almacenada en la memoria de un dispositivo, como las computadoras,

[2] Si bien los casos abundan en ambas circunstancias, a modo ejemplificativo cabe mencionar, en cuanto a espionaje gubernamental, la reciente investigación del Citizen Lab (Universidad de Toronto) sobre malware utilizado contra un defensor de derechos humanos en los Emiratos Árabes Unidos, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender", https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/; así como también las revelaciones de la empresa italiana Hacking Team, distribuidora de spyware, "Hacking Team en América Latina: El negocio de espiar a las personas" (por Derechos Digitales), https://www.derechosdigitales.org/wp-content/uploads/HT-mapa.png. En cuanto al sector empresarial, la gran mayoría que presta servicios en internet, desde emails hasta redes sociales, basan sus modelos de negocios en la recolección de información de sus usuarios para comercializar con terceros (generalmente redes publicitarias). En tal sentido, el "internet de las cosas" presenta nuevos desafíos para la privacidad, como ocurrio con ciertos televisores de Samsung y su reconocimiento de voz: "Samsung's warning: Our Smart TVs record your living room chatter" (Advertencia de Samsung: Nuestros Smart TV graban la charla en su sala de estar), CNET, https://www.cnet.com/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/

[3] OECD Guidelines for Cryptography Policy ("Guía de la OCDE para políticas sobre cirptografía"), 1997, http://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm

smartphones, tablets, flash drives o memorias USB, es cifrada mientras reside en dicho dispositivo. Sistemas operativos como las distribuciones GNU\Linux, Mac OS, iOS (iPhone, iPad), y Android, ofrecen opciones para cifrar la información almacenada en sus correspondientes dispositivos (algunos por defecto, otros seleccionando la opción al momento de configurar el sistema operativo por primera vez). En el caso de Microsoft, si bien ofrece en Windows 10 una opción para cifrar el disco donde se encuentre instalado el sistema operativo, el usuario debe utilizar una Cuenta Microsoft, ya que Windows sube las llaves privadas de cifrado a sus servidores en el caso que la persona no pueda ingresar a su computadora y necesite recuperar archivos, lo cual implica que estas claves también pueden verse comprometidas a solicitudes por agencias de inteligencia, fuerzas de seguridad, policías y fiscalías. Microsoft ofrece otra herramienta conocida como BitLocker, pero tan solo se encuentra disponible en las versiones profesionales/corporativas de Windows.

Cifrado punto a punto (o *end-to-end encryption*): es el proceso por el cual se cifra la información para ser enviada desde el punto A al punto B de manera tal que ninguno de los intermediarios de esa transferencia –como por ejemplo la empresa que brinda el servicio de mensajería o incluso el proveedor de servicio de internet (ISP, por sus siglas en inglés)– pueda ver el contenido de la información, ni que terceros que puedan interceptar la transferencia puedan acceder al mismo. El cifrado punto a punto lo encontramos hoy en día en aplicaciones de mensajería como Signal,[4] WhatsApp,[5] iMessage,[6] Allo,[7] Facebook Messenger[8] y Telegram[9] (aunque estas tres últimas no lo tienen activado por defecto en la configuración), así como también en tecnologías para asegurar emails, como PGP.[10]

Cifrado en la capa de transporte (o *transport layer encryption*): es el proceso por el cual se codifica la información entre el navegador y el sitio web que se quiere acceder, por ejemplo, asegurando que los datos de usuario y contraseña para iniciar sesión o de la tarjeta de crédito al realizar un pago, permanezcan ilegibles para quienes intermedien en la transmisión hasta llegar al servidor del sitio web. Esta forma de cifrado la encontramos presente en sitios web

[4] https://whispersystems.org

[5] "WhatsApp's Signal Protocol integration is now complete", Open Whisper Systems, abril 2016, https://whispersystems.org/blog/whatsapp-complete/

[6] iOS Security Guide, Apple, mayo 2016, https://www.apple.com/business/docs/iOS_Security_Guide.pdf

[7] "Open Whisper Systems partners with Google on end-to-end encryption for Allo", Open Whisper Systems, mayo 2016, https://whispersystems.org/blog/allo/

[8] "Messenger Secret Conversations: Technical Whitepaper", Facebook, julio 2016, https://fbnewsroomus.files.wordpress.com/2016/07/secret_conversations_whitepaper-1.pdf

[9] "Secret Chats, end-to-end encryption", Telegram, https://core.telegram.org/api/end-to-end

[10] PGP por las siglas en inglés de "Pretty Good Privacy", más información: https://en.wikipedia.org/wiki/Pretty_Good_Privacy

que utilicen HTTPS[11] (sea a través de TLS[12] o SSL[13]).

III ¿Dónde confluyen el cifrado y los derechos humanos?

Vimos hasta ahora que el cifrado es una tecnología que ayuda a mantener segura nuestra información, sea mientras transita por internet o cuando se encuentra almacenada en nuestros dispositivos, evitando que esos datos puedan ser accedidos por personas ajenas al intercambio de la información.

Es gracias a esta función en particular que podemos establecer que el cifrado nos ayuda a preservar y potenciar el goce de derechos humanos en la era digital. La privacidad, la libertad de expresión y opinión, la libertad de pensamiento, la libertad de reunión y asociación, son algunos de los principales derechos que debido al cifrado pueden ser ejercidos plenamente con las tecnologías que día a día son desarrolladas e implementadas.

El cifrado permite crear una zona de privacidad para proteger nuestras opiniones y creencias, así como también ejercer la libre expresión, evitando las injerencias y ataques de terceros, además de resguardarnos contra el cibercrimen y los abusos de gobiernos alrededor del mundo.

Como bien lo menciona el experto en criptografía y seguridad informática Bruce Schneier, "el cifrado es la tecnología más importante para preservar nuestra privacidad, y es especialmente adecuada para proteger contra la vigilancia masiva que llevan a cabo los gobiernos que buscan controlar a sus poblaciones y los criminales que buscan víctimas vulnerables (. . .)".[14]

La Asamblea General de las Naciones Unidas ha reafirmado que la privacidad es un derecho que habilita el goce de otros derechos, particularmente la libertad de expresión y la libertad de opinión, además de ser la base de una sociedad democrática.[15] Proteger el derecho a la privacidad implica a su vez salvaguardar un gran abanico de derechos que éste habilita.

La seguridad que brinda el cifrado puede jugar un rol fundamental en el desarrollo de nuestra personalidad como individuos, como bien lo menciona el Relator Especial para la Promoción y

[11] HTTPS, o Hypertext Transfer Protocol Secure, es la versión segura de HTTP ("protocolo de transferencia de hipertexto"), el protocol utilizado para transmitir información entre el navegador y el sitio web al que se quiera conectar. Cuando una página web utiliza HTTPS, los navegadores generalmente muestran un candado al lado de la URL.

[12] Transport Layer Security (TLS, o en español "seguridad de la capa de transporte"). Para más información leer: "HTTP Over TLS" ("HTTP sobre TLS"), Internet Engineering Task Force, RFC2818, mayo 2000, https://tools.ietf.org/html/rfc2818

[13] Secure Sockets Layer (SSL, o en español "capa de puertos seguros"). Para más información leer: "Difference between SSL & TLS" ("Diferencia entre SSL y TLS"), Stack Overflow, http://stackoverflow.com/questions/3690734/difference-between-ssl-tls

[14] "Why We Encrypt" ("Por qué ciframos"), Bruce Schneier, junio 2015, https://www.schneier.com/blog/archives/2015/06/why_we_encrypt.html

[15] Resolución 68/167, Asamblea General de la Organización de las Naciones Unidas, https://ccdcoe.org/sites/default/files/documents/UN-131218-RightToPrivacy.pdf

Protección del Derecho a la Libertad de Opinión y Expresión de las Naciones Unidas, David Kaye, "La posibilidad de navegar la web, desarrollar ideas y comunicarse en forma segura es tal vez la única manera en que muchas personas pueden explorar aspectos básicos de identidad, como su género, religión, etnia, nacionalidad y sexualidad".[16]

En Argentina, la Constitución Nacional consagra en su artículo 19 que "Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. (...)", mientras que en el artículo 18 se establece que "(...) El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación (...)"; estableciendo así las bases del respeto a la privacidad de los individuos, aún sin mencionarla explícitamente.

En su artículo 75, inciso 22, la Constitución incorpora tratados internacionales de derechos humanos otorgándoles jerarquía constitucional (ergo, superior a las leyes). Estos tratados consagran los principales derechos que se encuentran vinculados con el cifrado, de los cuales es menester destacar: la Declaración Universal de Derechos Humanos,[17] que consagra en su artículo 12 el derecho a la privacidad, en el 18 la libertad de pensamiento, en el 19 la libertad de opinión y expresión, y en el 20 la libertad de reunión y asociación; y concordantemente los artículos 17, 18 y 19 del Pacto Internacional de Derechos Civiles y Políticos;[18] los artículos 11, 13, 15 y 16 de la Convención Americana sobre Derechos Humanos;[19] así como los artículos 4, 5, 6, 9 y 10 de la Declaración Americana de los Derechos y Deberes del Hombre.[20]

En tal sentido, no podemos dejar de mencionar lo establecido por el Consejo de Derechos Humanos de la ONU en el año 2012, afirmando que "los mismos derechos que las personas tienen offline también deben ser protegidos online, en particular la libertad de expresión, que es aplicable independientemente de las fronteras y a través de cualquier medio que se elija (...)",[21] lo cual fue posteriormente reafirmado por la Asamblea General en el año 2014, mencionando específicamente

[16] Reporte del Relator Especial para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, ONU, A/HRC/29/32, 2015, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A_HRC_29_32_en.doc

[17] Declaración Universal de Derechos Humanos, Organización de las Naciones Unidas (ONU), 1948, http://www.un.org/es/universal-declaration-human-rights/

[18] Pacto Internacional de Derechos Civiles y Políticos, Organización de las Naciones Unidas (ONU), 1976, http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

[19] Convención Americana sobre Derechos Humanos, Organización de los Estados Americanos (OEA), 1969, http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm

[20] Declaración Americana de los Derechos y Deberes del Hombre, Comisión Interamericana de Derechos Humanos, OEA, 1948, http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp

[21] Resolution 20/8, "The promotion, protection and enjoyment of human rights on the Internet", Human Rights Council, 2012, https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement

el derecho a la privacidad.[22]

IV El cifrado alrededor del mundo

Desde hace varios años vemos casos de gobiernos alrededor del mundo argumentando la pérdida de poderes de investigación para prevenir e investigar actividades delictivas, como terrorismo, narcotráfico, trata de personas, y secuestros, por nombrar algunos.

Uno de los casos más paradigmáticos de los últimos años, y el más relevante para esta temática durante 2016, fue aquel entre el FBI y Apple en Estados Unidos a comienzos del 2016. A raíz de un atentado terrorista en San Bernardino, California, en el cual se recuperó un iPhone 5C que pertenecía a uno de los perpetradores, el FBI solicita a un juez que libre una orden para que Apple los ayude a ingresar al teléfono, el cual se encontraba protegido por un código de acceso (PIN numérico). Apple argumentó que el FBI estaba buscando el desarrollo de una versión de su sistema operativo que pondría en riesgo a millones de personas que utilizan sus dispositivos en todo el mundo, al pedirles la implementación de una puerta trasera (backdoor) en su software que permitiría romper el cifrado con el que se protege la información almacenada.[23]

Las organizaciones defensoras de derechos humanos EFF, ACLU, y Access Now, determinaron en un comunicado conjunto que el precedente buscado por el FBI "crea una nueva vía para que el gobierno reclute a empresas privadas para que construyan herramientas de vigilancia. Si Apple puede ser obligado a crear una llave maestra para desbloquear este iPhone, poco impedirá que el gobierno ordene a cualquier empresa que convierta sus productos en herramientas de vigilancia, comprometiendo la privacidad y seguridad de todos".[24]

Tras varias semanas en los tribunales, el FBI finalizó el litigio con Apple tras anunciarle al juez que había encontrado una manera de ingresar al iPhone en cuestión, por lo que ya no requería la asistencia de la empresa,[25] sobre lo cual se supo tiempo después que el FBI había pagado más de un millón de dólares por una vulnerabilidad que les permitía ingresar al iPhone 5C.[26]

[22] Resolución 68/167, p.2, Asamblea General, ONU.

[23] "The Fight For Encryption in 2016" ("La batalla por el cifrado en 2016"), Kurt Opsahl, EFF (Deputy Executive Director), 33th Chaos Communication Congress, https://youtu.be/H-xm5268GE4

[24] "The Apple Fight Is About All of Us" ("La batalla de Apple es sobre todos nosotros"), EFF, ACLU, Access Now, marzo 2016, https://www.eff.org/deeplinks/2016/03/apple-fight-about-all-us

[25] "U.S. Says It Has Unlocked iPhone Without Apple" ("Estados Unidos dice que logró desbloquear el iPhone sin Apple"), Katie Benner, Eric Lichtblau, New York Times, marzo 2016, http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0

[26] "FBI Paid More Than $1 Million to Hack San Bernardino iPhone" ("FBI pagó más de 1 millón de dólares para hackear el iPhone de San Bernardino"), Devlin Barret, Wall Street Journal, abril 2016, http://www.wsj.com/articles/comey-fbi-paid-more-than-1-million-to-hack-san-bernardino-iphone-1461266641

Luego de los atentados terroristas en París y Bruselas, las autoridades francesas y belgas argumentaron la necesidad de mayores facultades de investigación para las fuerzas de seguridad y las agencias de inteligencia, aún cuando luego se determinó que los actores del ataque en París planearon el atentado "a simple vista",[27] y que la computadora de uno de los perpetradores en Bélgica contenía los planes del ataque en una carpeta sin cifrar.[28]

Una vez más, estos casos demostraron una falencia latente en el trabajo que llevan a cabo las fuerzas de seguridad y las agencias de inteligencia, más que un problema vinculado con el uso de determinadas tecnologías. Gracias a que en los últimos años se ha ido abaratando el costo del desarrollo tecnológico, y consecuentemente las herramientas de vigilancia, países como Estados Unidos y el Reino Unido se han preocupado en poner en funcionamiento sistemas de vigilancia masiva indiscriminada, surtiendo como efecto que este tipo de casos puedan pasar prácticamente desapercibidos en la masiva cantidad de información recolectada.

En algunos países ya se han aprobado leyes e implementado regulaciones que directamente limitan o prohíben el uso de herramientas de cifrado, o incluso se han popularizado prácticas que ponen en riesgo a la ciudadanía y generan precedentes que quedan fuertemente arraigados en la cultura judicial.

En el Reino Unido, Francia, y España, el gobierno puede solicitar a las compañías las llaves privadas para descifrar la información.[29]

De acuerdo a un reciente reporte de Amnesty International, "países como Pakistán, India y Cuba prohíben el cifrado, restringen la fuerza del cifrado legal a los niveles establecidos por el gobierno, o exigen a las personas que soliciten autorización para utilizar cifrado",[30] mientras que Turquía "requiere que los distribuidores de cifrado provean las llaves privadas a los entes reguladores antes de brindar las herramientas de cifrado a los usuarios".[31]

En Colombia, el cifrado se encuentra regulado por ley, por un lado, los operadores de telecomunicaciones solo pueden ofrecer el servicio de cifrado a ciertos funcionarios del gobierno, además de estar

[27] "Paris Attacks Plot Was Hatched in Plain Sight" ("Ataques en París organizados a simple vista"), Stacy Meichtry, Joshua Robinson, Wall Street Journal, http://www.wsj.com/articles/paris-attacks-plot-was-hatched-in-plain-sight-1448587309

[28] "Brussels Terrorist Laptop Included Details Of Planned Attack In Unencrypted Folder Titled 'Target'" ("La laptop del terrorista en Bruselas incluía detalles del ataque en una carpeta sin cifrar nombrada 'Objetivo'"), Mike Masnick, Techdirt, abril 2016, https://www.techdirt.com/articles/20160413/17113634175/brussels-terrorist-laptop-included-details-planned-attack-unencrypted-folder-titled-target.shtml

[29] En Reino Unido: Regulation of Investigatory Powers Act, http://bit.ly/2hRLmIX; en Francia: Ley 2001-1062 de "Seguridad Cotidiana", http://bit.ly/2id3hgh; en España: Ley de Telecomunicaciones 25/2007, http://bit.ly/2iKc22g

[30] "Encryption: A Matter of Human Rights", Amnesty International, marzo 2016, p.12, https://www.amnestyusa.org/research/reports/encryption-a-matter-of-human-rights

[31] Íbid.

prohibido el envío de mensajes cifrados y en clave.[32]

En Brasil, en tres ocasiones entre fines de 2015 y mediados de 2016,[33] distintos jueces ordenaron bloquear a nivel nacional la aplicación de mensajería WhatsApp (de Facebook, Inc.), debido al incumplimiento de las correspondientes órdenes judiciales por parte de la compañía, las cuales los obligaba a facilitar los mensajes enviados por un grupo de usuarios vinculados a investigaciones penales, aún a pesar que la compañía había aclarado a los magistrados su imposibilidad de cumplir con la medida debido a que ellos no tienen acceso al contenido de los mensajes gracias al protocolo de cifrado implementado. De esta forma, el poder judicial brasilero dejó sentado un peligroso precedente, contrario a los principios de necesidad y proporcionalidad,[34] no solo para Brasil, sino para toda la región.

V Seguridad para todos

A raíz de todo lo expuesto anteriormente, queda claro que el cifrado es uno de los pilares fundamentales no solo para el goce y ejercicio de derechos humanos, sino también que como resultado de ello es que se logra amparar el pleno desarrollo de una sociedad libre y democrática.

A grandes rasgos, el cifrado permite a profesionales cumplir con su deber de reserva y confidencialidad, como en el caso de los abogados y contadores con sus clientes, así como de médicos, psicólogos y profesionales de la salud que deben trabajar con información privada de sus pacientes.

El cifrado ayuda a periodistas a preservar la identidad de sus fuentes y asegurar la información que los mismos les facilitan, evitando que la misma pueda ser adulterada o robada. Entre los casos mundiales más paradigmáticos en los últimos años cabe mencionar las revelaciones de Edward Snowden,[35] WikiLeaks,[36] y Panama Papers,[37] en los cuales el cifrado jugó un rol primordial con el fin último de llevar la información a conocimiento del público.

El cifrado protege la infraestructura de los gobiernos y empresas. Asegura que servicios críticos como la luz, el agua, el gas, el transporte, las comunicaciones, permanezcan en constante funcionamiento.

[32] "La peligrosa ambigüedad de las normas sobre cifrado de comunicaciones en Colombia", Juan Diego Castañeda, enero 2015, http://www.digitalrightslac.net/es/la-peligrosa-ambiguedad-de-las-normas-sobre-cifrado-de-comunicaciones-en-colombia/

[33] Diciembre 2015: http://www.lanacion.com.ar/1855037-whatsapp-bloqueo-brasil-telefono; mayo 2016: http://www.lanacion.com.ar/1894716-justicia-brasil-bloqueo-whatsapp; julio 2016: http://www.lanacion.com.ar/1919912-una-jueza-bloqueo-whatsapp-en-brasil-porque-facebook-no-le-entrega-una-serie-de-mensajes-de-presuntos-delincuentes

[34] Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones: https://necessaryandproportionate.org/es/necesarios-proporcionados

[35] Para más información ver: https://edwardsnowden.com/revelations/; http://bit.ly/2dwNPcx; https://en.wikipedia.org/wiki/Edward_Snowden.

[36] https://wikileaks.org/

[37] https://panamapapers.icij.org/

El cifrado permite a la sociedad civil, organizaciones no gubernamentales (ONGs) y activistas, resguardar su trabajo y la confidencialidad de las personas con quienes trabajan, sobre todo en temáticas sensibles como la violencia de género, el aborto, la violencia institucional, la corrupción y el abuso de poder, además de a su vez proteger la integridad física de las personas involucradas, especialmente en países bajo regímenes autoritarios.

A comienzos de 2016, la organización internacional Access Now lanzó una coalición global, de la cual la ADC forma parte, con el fin de instar a los gobiernos alrededor del mundo a proteger y potenciar el desarrollo del cifrado y tecnologías derivadas, bajo el lema "Seguridad para todos".[38]

La campaña busca alentar a los líderes mundiales a apoyar la seguridad de las personas, las empresas y los mismos gobiernos, rechazando leyes, políticas y prácticas que pongan en peligro, socaven o limiten el acceso y desarrollo del cifrado y demás herramientas y tecnologías de comunicación segura. En la carta firmada por organizaciones, empresas e individuos de todas partes del mundo, se establecen cinco puntos principales:

- "Los gobiernos no deberían prohibir ni limitar el acceso de los usuarios a las tecnologías de cifrado; o prohibir el uso de cifrado por grados o tipos;
- Los gobiernos no deberían exigir el diseño o la implementación de 'puertas traseras' (*back-doors*) o vulnerabilidades en herramientas, tecnologías o servicios;
- Los gobiernos no deberían requerir que las herramientas, tecnologías o servicios sean diseñados o desarrollados para permitir el acceso de terceros a datos sin cifrar o a las claves de cifrado;
- Los gobiernos no deberían tratar de debilitar o socavar los estándares de cifrado o influir intencionalmente en su desarrollo, a menos que sea para promover un mayor nivel de seguridad de la información.
- Ningún gobierno debería exigir algoritmos, estándares, herramientas o tecnologías de cifrado inseguros. Tampoco debería, por acuerdo privado o público, obligar o presionar a entidades para que actúen de manera incompatible con los principios anteriores."

Los sucesos ocurridos en los últimos años, algunos brevemente expuestos en este informe, dan cuenta de una creciente tendencia mundial que pretende enmarcar el debate entre seguridad y privacidad desde un punto de vista de tipo suma cero: si tenemos uno, no podemos tener completamente el otro, necesariamente hay que ceder en algún grado. Este argumento expuesto por las fuerzas de seguridad y las agencias de inteligencia no hace más que sesgar el debate para la opinión pública,

[38] "Announcing a global coalition demanding security for all", Access Now, enero 2016, https://www.accessnow.org/announcing-a-global-coalition-demanding-security-for-all/ Más información en https://securetheinternet.org

dejando de lado todos los matices que debemos considerar al momento de analizar cualquier medida y política pública, aún más cuando hay tecnología involucrada.

Desde la ADC estaremos atentos a las iniciativas nacionales y regionales que puedan debatirse en los espacios legislativos, así como también seguiremos con atención las políticas que sean propuestas o implementadas por las fuerzas de seguridad y las agencias de inteligencia, puesto que para la defensa de los derechos humanos en juego, es fundamental preservar los principios de proporcionalidad y necesidad ya mencionados.


por los Derechos Civiles