Informe regional sobre políticas y libertades en el uso del cifrado en América Latina y el Caribe

Ejecución

Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec
Derechos Digitales

Autores

Abdías Zambrano
Alejandro Moreno Baquero
Alex Renan de Sousa Galvão
Iago Capistrano Sá
Isabelle Brito Bezerra Mendes
João Araújo Monteiro Neto
Larissa Rocha
Letícia Alves
Lia Hernández
Lucas Domínguez Rubio
Luis Henrique de Menezes Acioly
Luiza Correa de Magalhães Dutra
Matheus Fernandes da Silva
Paulo Rená da Silva Santarém
Rómulo Chacín González
Victor Barbieri Rodrigues Vieira
Wilson Guilherme Dias Pereira

Coordinación y Revisión

Mariana Canto
Raquel Saraiva
Michel Souza

Traducción

Fernanda Lobo

Idealización

André Ramiro

Proyecto grafico

Clara Guimarães

IP.rec usó recursos de WhatsApp LLC. para producir este informe.

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Informe regional sobre políticas y libertades en el uso del cifrado en América Latina y el Caribe [livro eletrônico] / coordenação Mariana Canto, Raquel Saraiva, Michel Souza ; tradução Fernanda Lobo. -- Recife, PE : IP.rec, 2023.
PDF

Vários autores.
Título original: Relatório regional sobre políticas e liberdades no uso de criptografia na América Latina e no Caribe.
ISBN 978-65-995947-8-6

1. Criptografia de dados (Computador) - Legislação 2. Marco Civil da Internet 3. Proteção de dados - Direito - Brasil 4. Segurança da informação I. Canto, Mariana. II. Saraiva, Raquel. III. Souza, Michel.

23-151925 CDU-342.721

Índices para catálogo sistemático:

1. Criptografia : Segurança : Direito civil 342.721
Tábata Alves da Silva - Bibliotecária - CRB-8/9253

Resumen

INTRODUCCIÓN

El debate sobre el cifrado en todo el mundo sigue enmarcándose como una tensión entre, por un lado, la seguridad de la información y la privacidad de las comunicaciones y, por otro lado, la accesibilidad para las investigaciones criminales y la aplicación de la ley y con fines de seguridad nacional. Buscando comprender cómo las coyunturas políticas relacionadas con el uso y desarrollo del cifrado han impactado los derechos en la región, el "Informe regional sobre políticas y libertades en el uso del cifrado en América Latina y el Caribe" expone el estado de las políticas públicas y el nivel de libertad sobre el uso de tecnologías criptográficas en la región.

Resultado de la alianza entre el Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec, a través del Observatorio de Criptografía - ObCrypto, y Derechos Digitales, la publicación tiene como propósito exponer, de manera no exhaustiva, los diferentes riesgos en los poderes legislativo, ejecutivo y judicial latinoamericano y caribeño para el uso y desarrollo de tecnologías con cifrado. Asimismo, ofrece un mapeo del estado de las libertades en torno al uso del cifrado en la región y un termómetro sobre el ejercicio de derechos conexos al pleno uso de la criptografía, tales como libertad de expresión, opinión, manifestación y asociación, privacidad, seguridad y protección de datos personales.

Así, el proyecto buscó articularse con diferentes relatores en países estratégicos de la región, incluyendo activistas, organizaciones dedicadas a la defensa de los derechos humanos en el contexto de las nuevas tecnologías, así como miembros de la academia e investigadores. Agradecemos los aportes realizados por nuestros relatores, sin los cuales este informe no sería posible, y quienes actuaron como especialistas necesarios para construir un panorama contemporáneo del escenario legislativo y judicial relacionado con el tema, así como de los hechos políticos y contextos de interés en la región.

Finalmente, con base en esta publicación, el objetivo es brindar los insumos necesarios para acciones de incidencia sobre situaciones que alertan sobre restricciones al uso civil de la criptografía, así como incentivar nuevas investigaciones sobre el tema desde una perspectiva latinoamericana y caribeña. Como resultado, el proyecto tuvo como objetivo crear un precedente documental de utilidad pública que refleje el estado de la garantía de los derechos humanos relacionados con el uso del cifrado en América Latina.

País: Argentina

Autor: Lucas Domínguez Rubio

Organización: Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET)
Centro de Documentación e Investigación de la Cultura de Izquierdas (CeDInCI)

Notas para una historia reciente de la difusión del cifrado en Argentina (2010-2020)

• Introducción

Este informe propone un recorrido por los diferentes espacios que promovieron el uso de GnuPG, OTR y TOR en Argentina o las discusiones alrededor de estas herramientas para el cifrado de correo electrónico, mensajería y navegación. Refiere entonces al uso de criptografía que no tiene que ser implementada directamente por las plataformas proveedoras de servicios digitales para garantizar la seguridad de datos, servicios o transacciones, sino a herramientas a ser usadas desde abajo por voluntad o necesidad de lxs propios usuarixs.

Probablemente fue alrededor del año 2010 cuando podemos registrar los primeros talleres y textos que comenzaron a buscar una difusión sistemática de estas herramientas y las discusiones que traen aparejadas. Diez años después, el cifrado de las comunicaciones en los servicios de mensajería mediante OTR quedó obsoleto. Aunque en el caso de las implementaciones privativas de cifrado punta a punta resulta imposible su auditoría, el uso masivo de los principales servicios de mensajería instantánea —como WhatsApp (Meta, ex Facebook) y, en menor medida, Telegram y Signal— hizo que el uso de OTR haya desaparecido totalmente de la discusión.[1]

En el caso de TOR, las discusiones se mantuvieron siempre a niveles mínimos y, aunque su utilización involucre discusiones y prácticas totalmente diferentes, la extensión de servicios de VPN se convirtió en una alternativa parcial a ser utilizadas con ciertos fines.[2] El número de nodos TOR en Argentina osciló entre 0 y 8 en los últimos diez años. En sus extremos, en el 2013 había ocho nodos de salida, en el 2017 había 0, y en noviembre del 2022 contamos con 8 nodos, de los cuales sólo 2 de ellos son de salida.[3] Ni su uso ni sus

1 Pasquali, M. (2021). Infografía: Telegram y Signal registran más descargas que WhatsApp en Latinoamérica. Statista Infografías. https://es.statista.com/grafico/23928/descargas-de-telegram-signal-y-whatsapp-en-latinoamerica/

2 Ramadhani, E. (2018). Anonymity communication VPN and Tor: A comparative study. Journal of Physics: Conference Series, 983(1), 012060. https://doi.org/10.1088/1742-6596/983/1/012060

3 https://nusenu.github.io/OrNetStats/w/ En este sentido, el uso de TOR en Argentina siguió la tendencia común que se dio a nivel a global registrando un pico en su uso a fines del 2013: https://metrics.torproject.org/userstats-relay-country.html?start=2010-08-23&end=2022-11-21&country=ar&events=off

discusiones tuvieron aquí mayores repercusiones, y sólo algunos casos puntuales llamaron la atención pública.[4]

Por su parte, si bien el correo electrónico constituye el medio más utilizado para las comunicaciones formales, las principales organizaciones activistas que impulsan estos temas no publican sus llaves públicas en sus páginas de contacto. Hoy en día el bajo uso de GnuPG se combina con nuevos modos de su implementación en servicios de correo electrónico basados en la privacidad (sobre todo Protonmail y Tutanota). Los eventos específicos para intercambiar y firmar mutuamente las respectivas llaves públicas de GnuPG —llamados criptoparties— se difundieron en Europa entre 2012 y 2019.[5] Si bien en ese mismo período en Argentina existieron también algunas crytoparties en donde además se debatía y difundía el uso de TOR y OTR, en un ciclo similar, hoy en día también se encuentran discontinuadas.[6]

• Metodología

Con el fin de lograr un "reporte regional sobre políticas y libertades en el uso del cifrado en América Latina" resulta fundamental conocer las publicaciones y los modos de difusión que tomó la promoción del uso de criptografía en Argentina. En este sentido, se adopta un enfoque basado en la historia editorial y los medios de difusión: talleres, libros, revistas y plataformas web que difundieron los problemas alrededor de la criptografía en los últimos años permiten reconocer discusiones comunes. ¿Cuáles fueron los espacios desde dónde se promovió el uso de criptografía a nivel personal? ¿Cuáles textos y autores se usaron para alentar este debate? ¿Es posible identificar estrategias locales específicas a nivel nacional? ¿Fueron debates que se dieron de manera aisladas o vinculados a otros temas?

• Contexto y antecedentes

Las publicaciones de las distintas plataformas relevadas muestran un arco de temas en común que circularon como intereses compartidos, sobre todo alrededor de dos ejes: privacidad/criptografía y software libre/licencias copyleft. Se trata de discusiones en buena medida internacionales producidas en la década en la que el uso de internet para todas las esferas de la vida dio un salto cuantitativo de enorme magnitud hasta volverse imprescindible. De modo que las plataformas locales de visibilización y discusión de estos problemas se inscribían en una agenda global de referencias, nombres y problemas de mayor escala. Frente al crecimiento del uso de servicios digitales mainstream y el avance pretendidamente neutral de la tecnología a nivel cotidiano, sólo unos pocos espacios buscaron politizar el uso de software para preguntarse por las alternativas que se abrían.

• La difusión del cifrado en Argentina

Si bien la Fundación Vía Libre fue creada en la ciudad de Córdoba en el año 2000, sus actividades tomaron visibilidad sobre todo a partir del año 2008 y se centralizaron en la ciudad de Buenos Aires. Sus intereses radicaron en la difusión del software libre y

4 Iglesias, R. & Barrera Oro, I. (2017). Tor Exit Nodes En La Justicia Argentina [Video]. https://archive.org/details/torexitnodesenlajusticiaargentina

5 Hyde, A. et. al. (2013) https://archive.org/stream/cryptoparty/cryptoparty_djvu.txt

6 Kannengießer, S. (2020). Reflecting and acting on datafication: CryptoParties as an example of re-active data activism. Convergence, 26(5–6), 1060–1073. https://doi.org/10.1177/1354856519893357 ; Monsees, L. (2020). Cryptoparties: Empowerment in internet security? Internet Policy Review, 9(4), 1–19. https://doi.org/10.14763/2020.4.1508

las licencias que potencien la circulación del conocimiento[7] junto con campañas contra el avance de la vigilancia y la pérdida de privacidad ciudadana, respecto a distintos temas que tomaron visibilidad, como la difusión de DRM (2008), el voto electrónico (2009 y 2016), el reconocimiento facial, y, más recientemente, la inteligencia artificial.

Se trata de hecho de la única organización que ha impulsado una tarea de difusión sistemática de largo aliento sobre estos temas a través de notas de prensa regulares en distintos medios.[8] Aunque no se hayan dedicado expresamente a la difusión al uso,,, de las herramientas de cifrado de las comunicaciones, contribuyó a generar una serie de discusiones mediante textos y autores que por lo general acompañaban el uso de las herramientas criptográficas mencionadas.

Probablemente una de las características particulares del contexto local fue la temprana creación de una revista autogestiva fuertemente política como En Defensa del Software Libre en la Buenos Aires del 2010. Aunque su radio de repercusión haya sido reducido, se trató de la tarea de introducción de una agenda propia de discusiones y autores que buscaba una politización inexistente en el país. Además de Richard Stallman —invitado por la Fundación Vía Libre a Argentina en dos ocasiones—, autores como Dmytri Kleiner, Eben Moglen, Maxigas, Evgeny Morozov, Johan Söderberg, Jakob Rigi y Michel Bauwen eran introducidos por primera vez en Argentina, tanto desde las páginas de la revista como desde su colección editorial.[9]

La diferencia específica de este proyecto radicaba en su vinculación directa a una cultura de izquierdas autónoma, desde las cuales propulsaban una agenda centrada en licencias copyfarleft (y no copyleft)[10], plataformas digitales horizontales y antijerárquicas (como Loomio) y una reflexión basada en las posibilidades de la producción de pares, incluso antes de la creación de la revista específica sobre el tema, Peer production (Países Bajos, 2012) donde evaluaban la promesa del p2p de un nuevo modo de organización del trabajo y su producción. Además desde aquí se impulsaron talleres dedicados especialmente a la difusión de OTR, GnuPG y TOR con una lectura política de estas herramientas, junto con la creación de talleres de instalación de GNU/Linux y herramientas de seguridad como Iptables.

Estos últimos proyectos estuvieron vinculados al derrotero local del Partido Interdimensional Pirata (PIP) organizado en Argentina también desde el año 2010. Iniciados cuatro años antes en el norte de Europa, los partidos piratas impulsaron sobre todo una agenda sobre derechos civiles, democracia directa, cultura libre, privacidad de la información, transparencia de la información, libertad de expresión y neutralidad de la red[11].

Por su parte, entre el 2014 y el 2017, la experiencia local alcanzó en su momento de mayor visibilidad unos doscientos miembrxs, durante los años en que también brindaron talleres de cifrado llamados Grog & Tor y charlas y cursos sobre privacidad y género, a la

---

7 Boyle J. Brand U. Busaniche B. Drossou O. Heinz F. Montesinos C. Mooney P. Poltermann A. & Rodríguez S. (2005). ¿Un mundo patentado? la privatización de la vida y del conocimiento (1. ed.). Fundación Vía Libre; Boyle J. (2006). Prohibido pensar propiedad privada: los monopolios sobre la vida el conocimiento y la cultura. Fundación Via Libre; Busaniche, B. et. al. (2007). MABI: monopolios artificiales sobre bienes intangibles. Córdoba : Fundación Vía Libre; Busaniche, B. (Ed.) (2010). Argentina copy-left: La crisis del modelo de derecho de autor y las prácticas para democratizar la cultura. La Plata: UNLP.

8 https://www.vialibre.org.ar Por ejemplo: Link1 ; Link2 Link3 ; Link4 ; Link5

9 https://endefensadelsl.org/

10 Kleiner, D. (2007/2013). El manifiesto telecomunista. Buenos Aires: EDSL.

11 Otjes, S. (2020). All on the same boat? Voting for pirate parties in comparative perspective. Politics 40 (1), 38-53. https://doi.org/10.1177/0263395719833274

par que desarrollaron la colección editorial Utopía Pirata. Sus publicaciones ya superan la treintena —con una docena de títulos como libros y folletos largos. Además de algunos textos programáticos para organizarse horizontalmente, esa colección introduce autores como David Graeber, Johan Söderberg, Rick Falkvinge, Gabriella Coleman, Starhawk, Amador Fernández-Savater y Aaron Swartz, mientras retoman para su agenda autorxs como Oscar Varsavsky, Murray Bookchin y Hakim Bey.[12]

Sobre todo en los últimos quince años existieron en Argentina diferentes proyectos vinculados a la conformación de redes libres de topología de malla (mesh). Basados en software libre, su objetivo general consiste en desplegar redes libres comunitarias de bajo costo, en muchos casos en zonas de difícil accesibilidad a servicios digitales. Si bien los proyectos más recientes fueron acompañados por diferentes ONG, desde el 2002 existieron proyectos de distinto éxito en Rosario, Mendoza, Córdoba, Buenos Aires y el delta de El Tigre.

En el caso del proyecto Buenos Aires Libre (2006), su principal objetivo fue lograr que la interconexión descentralizada que deje de depender exclusivamente de las grande compañías. Aunque muchas de ellas se encuentran hoy en día discontinuadas, siguen siendo una opción para espacios de difícil acceso[13]. Una vez más, la importancia de estos emprendimientos colectivos obtienen una importancia primordial, altamente productiva, al momento de generar comunidad y discusiones al rededor de una internet anti-jerárquica, libre, independiente y crítica de la centralización de los servicios, así y todo, las herramientas criptográficas mencionadas como eje de este informe no forman parte de sus programas. Hoy en día se trata de proyectos impulsados sobre todo por Libre Router y Alter Mundi con publicaciones sobre el tema.[14]

Como en todo el mundo, el movimiento alrededor del software libre generó no sólo grupos de soporte sino además activistas, entusiastas, cooperativas de trabajo, militancias, organizaciones, grupos de contacto en diferentes redes sociales y canales de mensajería y conferencias. En este sentido, sólo algunas obtuvieron prevalencia en el tiempo promoviendo una agenda cultural.

Entre las conferencias, cabe destacar el evento anual llamado Festival Latinoamericano de Instalación del Software Libre (FLISOL) que, a través de sus programas, en cada una de sus ediciones, se convirtió en el espacio de numerosos talleres vinculados a la criptografía y a la privacidad, por ejemplo: sobre la utilización de servidores propios, el funcionamiento y el uso de TOR y OTR, la propagación de servicios de mensajerías federados y autónomos, la importancia de usar estas herramientas y muchas otras cosas más[15]. En menor medida, algunas cooperativas de trabajo de desarrollo de software dieron lugar a talleres sobre comunicaciones seguras[16].

Al hablar de hacklabs y hackerspaces, partimos de la diferenciación realizada por Maxigas,[17] quien propuso pensarlos como dos genealogías. Según este texto los llamados hackerspaces se vinculan a una tradición californiana, como espacios neoliberales de

12 https://utopia.partidopirata.com.ar

13 Prato, A., Weckesser, C. y Segura, M. (2020). AlterMundi y la primera red comunitaria de Internet cien por ciento LibreRouter. Córdoba: UNC.

14 https://librerouter.org/ ; https://altermundi.net/

15 Pueden consultarse los programas de las últimas ediciones: https://flisol.info/

16 https://facttic.org.ar/category/software-libre/ ; https://www.gcoop.coop/

17 Maxigas [seud.] (2015). Hacklabs y Hackerspaces: rastreando dos genealogías. En Defensa del Software Libre 3. https://endefensa-delsl.org/hacklabs-y-hackerspaces.html

discusión e innovación tecnológica financiados por grandes empresas. Mientras los hacklabs se organizarían sobre una cultura autonomista y autogestiva. Para el caso argentino, o mejor dicho, de Buenos Aires, esta distinción resulta por demás adecuada, y, de hecho, los tres hacklabs que funcionaron y funcionan, fueron espacios desde los cuáles, de distintos modos, se difundió el uso de criptografía para las comunicaciones personales. El hacklab de Barracas funcionó entre entre el 2012 y el 2016, con miembxs vinculados tanto al Partido Pirata de Argentina —PIP— como a la publicación En Defensa del Software Libre —EDSL. En la misma dirección, fue uno de los pocos espacios que organizó crytoparties, es decir, eventos destinados a intercambiar y firmar las respectivas llaves públicas GnuPG en conjunción con otros talleres de seguridad. Tras su cierre, algunxs de sus miembrxs formaron el hacklab Rlyeh en 2017 sin la participación del Partido Pirata local.[18] Además, entre 2012 y 2017 existió un hacklab menos activo en la ciudad de Mar del Plata.[19]

El Centro Cultural Tierra Violeta, vinculado a la Red Argentina de Género, Ciencia y Tecnología (RAGCYT) fundada en el 2011, fue otro espacio especialmente abierto a talleres sobre género, tecnología, defensa digital y herramientas de cifrado. Al menos desde el 2012 existieron aquí varios talleres feministas de autodefensa digital.[20] Además, entre el 2016 y el 2019 se llevó a cabo mensualmente el evento Hacklab Violeta o Grog & Torta, definido como un "taller feminista de autodefensa digital" y también impulsado por el PIP.

Fuera del circuito mencionado hasta ahora, los libros y autorxs que circularon con cierta repercusión pertenecen a un espectro más amplio que puede pensarse común al ámbito internacional. La traducción de Cypherpunks —de Julian Assange, Jacob Appelbaum, Andy Müller-Maguhn y Jéremie Zimmermann— fue publicada en 2013, sólo un año después de su versión original en inglés, al igual de como sucedió con Cuando Google conoció Wikileaks.[21] Más allá de la introducción-manifiesto a favor de las "armas" criptográficas, la edición hispana resultaba más interesante por agregar una nota crítica no sólo a la vigilancia estatal, hacia PRISM y su vínculo con la NSA, sino sobre todo a la vigilancia empresarial alrededor de PRISM. Con todo, el libro careció de mayores repercusiones locales, las cuales casi únicamente estuvieron a cargo del periodista Santiago O'Donnell. Tras las revelaciones de Snowden algunas discusiones parecían tomar un revuelo, pero esto no se tradujo a nivel global en un aumento significativo del uso de criptografía.[22]

Podemos pensar que el circuito descrito fue también el que recuperó en Argentina sus repercusiones. En este ámbito, las periodistas que agarraron temas alrededor en los años posteriores fueron Natalia Zuazo[23] y Marta Peirano[24]. Entre estos, sólo este último libro con prólogo de Snowden se proponía confeccionar una "introducción a la criptografía para redacciones, whistleblowers, activistas, disidentes, y personas humanas en general": argumentando a favor del uso de estas herramientas. Dentro de este espectro vinculado a los libros, publicistas y activistas, otro eje a tener en cuenta al momento es el de lxs visitantes extranjeros. Entre ellxs, Richard Stallman, Jéremie Zimmerman, Marta Peirano y Renata Ávila

18 https://git.rlab.be/rlyehlab

19 https://twitter.com/mateslab?lang=en; https://sites.google.com/site/mateslaboratory/home

20 Avolio, M. (2017). Hacklab Violeta: Talleres para que las mujeres sepan cuidarse en Internet. Medium. https://kbz.red/hacklab-violeta-talleres-para-que-las-mujeres-sepan-cuidarse-en-internet-13629880bcb2

21 Assange, J., Appelbaum, J., Müller-Maguhn, & Zimmermann, J. (2013). Cypherpunks: la libertad y el futuro de internet. Barcelona, Deusto; Assange J. (2016). Cuando google encontró a wikileaks. Buenos Aires: Capital Intelectual.

22 Preibusch, S. (2015), Privacy Behaviors After Snowden. Communications of the ACM, 58 (5).

23 Zuazo N. (2015). Guerras de internet : un viaje al centro de la red para entender cómo afecta tu vida. DEBATE; Zuazo N. (2018). Los duenos de internet : como nos dominan los gigantes de la tecnologia y que hacer para cambiarlo. DEBATE.

24 Peirano, M. (2015). El pequeño libro rojo del activista en la red. Barcelona, Roca.

visitaron la Argentina en los años abordados, por lo general con invitaciones vinculadas a los grupos, asociaciones y hacklabs ya mencionados.

Finalmente, mencionaremos algunas editoriales que dieron a conocer una serie de textos alrededor de estos debates con una propuesta de intervención más teórica. En este sentido, la editorial Heckt editó una temprana compilación de textos sobre activismos digitales[25] y las traducciones de los textos de los colectivos Tiqqun[26] y Comité Invisible[27], con aproximaciones a la cibernética desde la filosofía francesa. En un sentido más amplio, la editorial Caja Negra desarrolla desde el 2014 una exitosa colección sobre nuevas tecnologías y políticas, traduciendo autores como Mark Fisher, Éric Sadin, Byung-Chul Han, y Nick Srnicek, entre otrxs. En esta dirección, el ámbito académico interesado por las izquierdas se enfoca sobre todo en perspectivas aceleracioncitas o la teoría crítica de la tecnología[28] alrededor de la revista Redes: revista de ciencias sociales, ciencia y tecnología (Bernal, 1997). El único evento académico dedicado específicamente a estas problemáticas con un impulso de difusión fue el realizado por la red de estudios sobre vigilancia Lavits (Latin American Network of Surveillance, Technology and Society Studies), que se fundó en 2009 dentro de la PUCPR - Pontifícia Universidade Católica do Paraná. (Curitiba, Brazil) y en el 2017 celebró su encuentro en en Buenos Aires.

De configuración más reciente, en el 2019 se creó el Observatorio de Derecho Informático Argentino (ODIA), orientado a problemáticas legales vinculadas a la informática, quienes en estos últimos años realizaron acciones alrededor de los programas de reconocimiento facial, el sistema de gestión de los casos judiciales utilizado en el país y la aplicación oficial que aquí se utiliza.[29] Sin tener tampoco un vínculo directo con la difusión de herramientas personales de cifrado, también en los últimos años tomó visibilidad Cybercirujas y su revista Replay, dedicada a la recuperación de equipos contra la obsolescencia programada.[30]

No vinculadas al ambiente académico, sino más bien técnico y profesional, podemos destacar las dos conferencias de seguridad informática Ekoparty (iniciadas en el 2002) y NotPinkCon, destinada a incrementar el interés de las mujeres y disidencias por la seguridad informática. Al tratarse de eventos técnicos tampoco se conformaron como un espacio de difusión del cifrado a nivel personal.

• Conclusión

En resumen, en buena medida, existe una difusión amplía del software libre, discusiones de licencia a través de distintos tipos de comunidades, así como también de seguridad o una discusión académica sobre tecnología sin que esto implique necesariamente una difusión de herramientas criptográficas. Probablemente un repaso de las agrupaciones que impulsaron discusiones y usos de las mencionadas herramientas criptográficas logre sólo una paneo

25 Lago Martínez, S. (2012). Ciberespacio y resistencias : exploración en la cultura digital (1ra edición). Hekht Libros.

26 Tiqqun (Collective) Sanromán Diego L & Rivera Parra C. (2013). Primeros materiales para una teoría de la jovencita. Hekht libros; Tiqqun (2001/2015). La hipótesis cibernética (R. Suárez y S. Rodríguez). Buenos Aires: heckt.

27 Comité Invisible. (2015). Carta a nuestros amigos. Buenos Aires: Hekht Libros; Avanessian, A. & Reis, M. (Comps) (2017). Aceleracionismo. Buenos Aires: Caja Negra.

28 Tula Molina, F. y Giulano, H. (2015). "La teoría crítica de la tecnología: revisión de conceptos", Redes 21 (41), 179-214 https://

29 odia.legal/

30 https://revistareplay.com.ar/

parcial sobre la situación en Argentina. Al centrarse en las publicaciones locales y dejar de lado comunidades digitales internacionales, esta perspectiva obtiene sus propios límites. Sin embargo, a partir del recorrido realizado, las siguientes consideraciones finales pueden proponerse para su debate.

• Recomendaciones

En primer lugar, resulta claro que las discusiones sobre la necesidad personal de cifrado no circularon aisladas, sino junto a otra serie de preocupaciones comunes que pueden organizarse en los siguientes ejes. (i) Privacidad de la información a nivel estatal y empresarial, junto a los peligros de la concentración de la información: en buena medida cristalizado a nivel global través de la importancia intencionalidad que tomaron los casos de Wikileaks, Assange, Maning, Snowden y Cambridge Analytics.[31] (ii) La discusión por las licencias, el acceso al conocimiento y los derechos de propiedad intelectual a partir de los nuevos modos de circulación de los bienes culturales: un debate iniciado por el software libre en la década del ochenta pero que obtuvo su repercusión alrededor de las discusiones por las leyes conocidas como el uso del P2P para el intercambio de música y películas y el impulso de las leyes PIPA y SOPA en los Estados Unidos (sobre todo entre 2011 y 2012) (Ariño, 2019). (iii) En menor medida, el optimismo del Software Libre y el P2P como modos de producción y difusión hacia una nueva organización del trabajo[32]; (iv) y la llamada gobernanza de internet llevada a cabo por distintas organizaciones para el establecimiento comunes de estándares.[33]

Sin embargo, en este último punto resulta necesario hacer una diferencia. Tanto a nivel internacional como local, las publicaciones relevadas muestran que los temas vinculados a la gobernanza han circulado por separado, y los grupos activistas que más impulsaron el uso de cifrado son escépticos sobre cualquier tipo de regulación, de ,,,,,modo que la única solución es implementar criptografía a nivel personal (esto puede verse claramente en Assange et. al., 2013, o a nivel local en las publicaciones del Partido Pirata).

Como sucede en muchos campos vinculados a la tecnología, se trata de un campo hegemonizado por varones cis, tanto a nivel local como internacional.[34] Con todo, puede pensarse que también los grupos activistas más autonomistas se han mostrado especialmente abiertos a discusiones y críticas alrededor del género.[35]

A nivel local, los datos con los que contamos y las plataformas de difusión identificadas hablan de un espacio de circulación reducido centralizado en Buenos Aires, con escasas referencias a las ciudades de Rosario, Córdoba y Mar del Plata. A nivel regional, el recorte de este informe que parte de un "nacionalismo metodológico" deja de lado algunas organizaciones de alcance regional con publicaciones que difundieron temas aledaños; como,

---

31 Spence E. H. (2021). Media corruption in the age of information. Springer. https://doi.org/10.1007/978-3-030-61612-0 Domínguez Rubio,

32 L. (2018). Izquierdas, software e internet: una agenda invisible. Nómadas, 54 (1). https://gitlab.com/Lucaslmdr/cv/-/blob/main/Lucas_Dom%C3%ADnguez_Rubio_-_izquierda__software_e_internet.pdf

33 Chenou, J.-M. (2021). Varieties of digital capitalism and the role of the state in internet governance: A view from Latin America. En Power and Authority in Internet Governance. Routledge.

34 Zukerfeld, M., Botta, M., Dughera, L. & Yansen, G., ¿Y las mujeres dónde están? Informe sobre género. Buenos Aires: Fundación Sa- Avolio, M. dosky.

35 (2017). Hacklab Violeta: Talleres para que las mujeres sepan cuidarse en Internet. Medium. https://kbz.red/hacklab-violeta-talleres-para-que-las-mujeres-sepan-cuidarse-en-internet-13629880bcb2

por ejemplo, la Alianza para el cifrado de América Latina y el Caribe (AC-LAC), fundada recientemente en 2021 con una agenda específica sobre el cifrado;[36] o la Asociación para el Progreso de las Comunicaciones (APC) fundada ya en 1990 con un alcance regional;[37] o Derechos Digitales, fundada en Chile en 2004, desde dónde se realizaron sus impresas, y que logró un alcance regional en los últimos años.

Por último, el segundo límite de este informe radica en su enfoque en las publicaciones realizadas sobre cifrado. Esto deja afuera una importante cantidad de talleres de seguridad realizados par activistas en riesgo, tanto en Argentina como otros países. Se trata de información que no es pública y funciona por canales acotados, sin embargo, constituyéndose como un modo fundamental de la difusión de las herramientas de cifrado: para activistas feministas a favor del aborto, comunidades indígenas del norte y el sur del país y movimientos campesinos. Rastrear únicamente lo publicado tiene este límite, así como también no ser un enfoque útil para atender urgencias de militancia más urgentes de seguridad física, donde, en un contexto de fuertes necesidades y conflicto, hablar de cifrado parece todavía un paso muy adelante y, antes que eso, resulta, por ejemplo, importante trabajar sobre la exposición en redes sociales.

36 https://ac-lac.org/

37 https://www.apc.org/es

País: Brasil

Autores: Luiza Correa de Magalhães Dutra, Paulo Rená da Silva Santarém, Victor Barbieri Rodrigues Vieira, Wilson Guilherme Dias Pereira

Organización: Instituto de Referência em Internet e Sociedade

Políticas públicas y movilizaciones sociales sobre cifrado en Brasil

• Introducción

En Brasil, algunas normas vigentes rozan el tema del cifrado: Marco Civil de Internet y respectivo decreto reglamentario, Ley General de Protección de Datos, Estrategia Nacional de Seguridad Cibernética y Política Nacional de Seguridad de la Información. Aunque no protejan expresamente el uso del cifrado, la ausencia de prohibición implica su autorización legal.

Amenazando tal escenario, propuestas legislativas pretenden imponer a proveedores de servicios cifrados obligaciones de rastreo, descifrado o custodia de llaves. Como contrapunto a tales peligros, iniciativas de la sociedad civil para la defensa, mantenimiento y difusión social de un cifrado fuerte en Brasil demuestran la importancia de movilizaciones de resistencia y presentan un campo más crítico a las iniciativas normativas para limitar el uso libre o incluso quebrar el cifrado.

En suma, a pesar de algunas graves situaciones de presión o cuestionamiento, persiste en el alcance normativo y jurisprudencial brasileño el apoyo al uso del cifrado, incluso sin garantía explícita, con respaldo de las organizaciones de la sociedad civil.

Esta publicación tiene como objetivo presentar la compleja situación actual de las políticas públicas y de las movilizaciones sociales sobre el cifrado en Brasil, ofreciendo un panorama de la legislación vigente, proyectos de ley, procesos judiciales, y campañas de movilización social, además de un diagnóstico de riesgos y amenazas al pleno ejercicio de derechos humanos pertinentes: libertades de expresión, de opinión, de manifestación y de asociación, privacidad, seguridad, y protección de datos personales.

• Metodología

La metodología utilizada se basó, en búsqueda de confiabilidad y densidad teórica, en la revisión sistemática de la literatura pertinente, con un recorte empírico en obras seleccionadas y evaluadas mediante criterios y procedimientos explícitos y

organizados, pasando por el mapeo del estado del arte sobre la situación legislativa y jurisprudencial del cifrado en Brasil, además de las movilizaciones civiles en el área. Para la investigación de la bibliografía se ha realizado un mapeo de obras relevantes que fueron utilizadas como puntos centrales en el reporte desarrollado.

En el ámbito legal, analizamos las principales normas vigentes relacionadas con el tema, mapeando protecciones jurídicas, autorizaciones legales de uso y posibles márgenes para acciones de amenazas. A partir de ese esquema, fue posible diagnosticar las propuestas legislativas y procesos judiciales que analizan actos represivos estatales para quiebra de cifrado y acceso a datos personales: la reforma del Código de Proceso Penal prevé la posibilidad de interceptación telemática; el PL 2518/2019 impone el monitoreo activo; el PL 2630/2020 exige la rastreabilidad de comunicaciones, aunque cifradas; entre otros proyectos de ley. Todavía, en el Supremo Tribunal Federal, a quienes cabe definir la interpretación de la Constitución Federal, hay riesgo de que el Poder Judiciario legitime la quiebra de cifrado en las acciones sobre bloqueos de WhatsApp (ADI 5527 e ADPF 403) y el acceso de autoridades policiales a dispositivos móviles durante flagrante (Tema de Repercusión General nº 977), para averiguación de la vida íntima y privada y acceso a datos personales, permitiendo investigaciones represivas, sin garantías legales y constitucionales.

Por fin, mapeamos las formas insurgentes de la sociedad civil frente a las amenazas analizadas. La Coalición Derechos en la Red organiza a la criptoAgosto desde el 2020, evocando el reconocimiento de la ancha importancia del cifrado. También emergieran las criptoFestas: iniciativas descentralizadas, difundidas por el mundo desde Australia. Variadas ediciones en Brasil constituyeron espacios de *artivisimo*, uniendo cultura, tecnología y política: CryptoRave en São Paulo, CriptoJP en Paraíba, CriptoBaião en Ceará, CriptoTrem en Minas Gerais, y CriptoFesta en Pernambuco. Todavía, hay esfuerzos internacionales, como el Dia Global de Criptografía y la organización de la Alianza para Criptografía en la América Latina y el Caribe.

De ese modo, la metodología adoptada crea un cuerpo analítico jurídico e institucional, desde bibliografías relevantes, que presenta el campo del cifrado en Brasil, con una mirada crítica para las evidencias y orientando investigaciones futuras.

• Contexto y antecedentes

Los intentos estatales y privados de contorneo del cifrado reflejan una compleja disputa mundial sobre este, objeto de variadas consideraciones por órganos de defensa de derechos humanos. En contextos bélicos, su valor informacional ofrece protección a las tácticas militares, beneficiando el poder público; pero al proteger la privacidad de particulares, es vista como un riesgo al Estado (especialmente en regímenes totalitarios, en donde la búsqueda por aplicaciones cifradas tiende a aumentar)[38].

De esa contraposición de perspectivas surgieron las llamadas *CryptoWars (*Guerras Criptográficas): conflictos entre sociedad civil y Estado, alrededor de la demanda por acceso excepcional de autoridades a puertas clandestinas, a pretexto de alejar los riesgos del cifrado para la seguridad pública, y, por otro lado, la demanda en el mercado de la privacidad por

38 Office of the High Commissioner for Human Rights. (2022). *The right to privacy in the digital age : report of the Office of the United Nations High Commissioner for Human Rights* (A/HRC/51/17). United Nations. https://digitallibrary.un.org/record/3985679?ln=en.

la elevación de la seguridad cifrada en productos comerciales. El conflicto tiene cuestiones perennes, todavía bajo disputa jurídica, tecnológica y argumentativa. Pero, históricamente, dos períodos son importantes: el final del siglo XX y el año del 2013, reconocidos por parte de la literatura como primera y segunda guerras criptográficas[39].

La primera *CriptoWars* empieza en el contexto de la II Guerra Mundial. Reduciendo la criptografía a su potencial militar, los EUA presionaron para restringir su uso fuera y dentro del país, imponiendo obstáculos a la exportación de tecnologías más avanzadas, y cohibiendo por la NSA la difusión doméstica[40]. La segunda posee trés eventos notorios. En el 2013, las denuncias de Edward Snowden, ex-integrante de la CIA e de NSA, sobre prácticas de cibervigilancia de los EUA[41] en contra de individuos y jefes de Estado.

Por fin, el último evento se refiere al caso Apple vs FBI, en el 2015[42], en que la autoridad investigativa buscó obligar la compañía a contornear el cifrado y proporcionar acceso al iPhone de un terrorista muerto, bajo alegación de seguridad nacional. El debate público se calentó, dándole fuerza a la disputa narrativa antagónica entre criptografía y seguridad pública.

En el contexto brasileiro, ese conflicto resultó en peleas judiciales envolviendo WhatsApp, entre el 2015 y el 2016, cuando la compañía resistió en suministrar acceso a datos de usuarios[43]. Fueron presentadas en el Supremo Tribunal Federal dos acciones de control concentrado de constitucionalidad, para "cuestionar la validez jurídica de las órdenes de bloqueo do WhatsApp ante la instancia máxima do Poder Judiciario brasileño, para que la decisión cree un mecanismo jurisprudencial que frene nuevos órdenes de bloqueo de la plataforma"[44].

De este modo, tanto cuanto los EUA, Europa, India y otros países que vivencian conflictos acerca del cifrado, Brasil hace su disputa en el contexto judicial y político, con un papel activo, incluso de la sociedad civil, como veremos en seguida.

• Políticas públicas y movilizaciones sociales sobre cifrado en Brasil

• La situación normativa del cifrado en Brasil

La utilización del cifrado como medio central para garantizar la seguridad en el medio

39 Pereira, A. B. G., Rodrigues, G. R., & Vieira, V. B. R. (2021). *Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise*. Instituto de Referência em Internet e Sociedade. https://bit.ly/3kGTde3.

40 Pereira, A. B. G., Rodrigues, G. R., & Vieira, V. B. R. (2021). *Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise*. Instituto de Referência em Internet e Sociedade. https://bit.ly/3kGTde3.

41 Pereira, A. B. G., Rodrigues, G. R., & Vieira, V. B. R. (2021). *Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise*. Instituto de Referência em Internet e Sociedade. https://bit.ly/3kGTde3.

42 Liguori Filho, C. A. (2020). Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate. *Michigan Telecommunications and Technology Law Review*, 26 (2), 317-345. https://doi.org/10.36645/mtlr.26.2.exploring

43 Pereira, A. B. G., Rodrigues, G. R., & Vieira, V. B. R. (2021). *Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise*. Instituto de Referência em Internet e Sociedade. https://bit.ly/3kGTde3

44 Pereira, A. B. G., Rodrigues, G. R., & Vieira, V. B. R. (2021). *Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise*. Instituto de Referência em Internet e Sociedade. https://bit.ly/3kGTde3

digital se ha ampliado en las últimas décadas.[45] Sin embargo, las controversias en torno a su uso circunscriben el campo. Instituciones de persecución penal explicitan la dificultad investigativa por el cifrado, lo que nombran "obscuridad" (*Going dark*), lo que volvería las comunicaciones digitales indescifrables para las autoridades policiales.

En Brasil, algunas normas airean el tema del cifrado, y rozan, de alguna manera, su importancia como aspecto técnico de salvaguarda a la integridad, confidencialidad, autenticidad y disponibilidad de datos digitales. El principio de la seguridad – previsto principiologicamente en el Marco Civil de Internet[46] al lado de otros derechos humanos pertinentes como ciudadanía, libre expresión, privacidad, protección de datos personales etc. – se densifica en el decreto regulador[47] con el deber de los proveedores de garantizar la inviolabilidad de datos vía "encriptación o medidas de protección equivalentes".

La Ley General de Protección de Datos,[48] en carácter ejemplar, pautada por la construcción de toda una cultura jurídica de conservación, al tratar de sigilo y seguridad exige "técnicas adecuadas que hagan los datos personales afectados ininteligibles (...) para terceros no autorizados a accederlos".

La Estrategia Nacional de Seguridad Cibernética[49] recomienda soluciones de cifrado para fortalecer la gobernanza; el uso social generalizado de recursos de cifrado para comunicación segura de asuntos sensibles; y el desarrollo de habilidades y soluciones en cifrado para incentivar investigación e innovación. Y la Política Nacional de Seguridad de la Información[50] comisiona a la alta administración de los órganos y entidades de la administración pública federal el rol de orientar programas, de proyectos y de procesos para "la utilización de recursos adecuados de cifrado a los grados de sigilo exigidos".

Ninguna de las normas vigentes prevé expresamente el derecho o la prohibición de un libre uso del cifrado. Por un lado, la ausencia de impedimento implica la autorización legal, a la luz del principio de la autonomía de la voluntad privada, destinadas a personas físicas y jurídicas. Pero, por otro lado, queda abierto el espacio para diversos tipos de abusos y excesos, que amenazan o restringen esa libertad.

---

45 Pereira, A. B. G., Rodrigues, G. R., & Vieira, V. B. R. (2021). *Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise*. Instituto de Referência em Internet e Sociedade. https://bit.ly/3kGTde3

46 Brasil. (2014). "Lei nº 12.965, de 23 de abril de 2014" (Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.). *D.O.U de 24/04/2014, pág. nº 1*. Alterada pela Lei nº 13.709, de 14/08/2018. *D.O.U de 15/08/2018, pág. nº 59.* http://www.planalto. gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.html

47 Brasil. (2016). "Decreto nº 8.771, de 11 de maio de 2016" (Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.). *D.O.U de 15/08/2018, pág. nº 59.* https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.html

48 Brasil. (2018). "Lei nº 13.709, de 14 de agosto de 2018" [Lei Geral de Proteção de Dados Pessoais (LGPD).]. *D.O.U de 24/04/2014, pág. nº 1*. Alterada pela Lei nº 14.460, de 25/10/2022. *D.O.U de 26/10/2022, pág. nº 3.* http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.html

49 Brasil. (2020). "Decreto nº 10.222, de 05 de fevereiro de 2020" (Aprova a Estratégia Nacional de Segurança Cibernética.). *D.O.U. DE 06/02/2020, P. 6.* https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.html

50 Brasil. (2018). "Decreto nº 9.637, de 26 de dezembro de 2018" (Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança na-cional.). *D.O.U de 27/12/2018, pág. nº 23.* Alterado pelo Decreto nº 10.222, de 05/02/2020. *D.O.U. DE 06/02/2020, P. 6.* https://www.planalto. gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.html

• Amenazas al cifrado en Brasil

En el ámbito privado, las recurrentes fugas de datos personales ilustran uno de los riesgos de la protección por cifrado todavía depender de la elección de compañías, frente a la incapacidad práctica de cualquier fiscalización por la Autoridad Nacional de Protección de Datos; y en el ámbito estatal, los problemas pueden ser identificados en los tres poderes.

En el Ejecutivo, sin iniciativas propositivas, como acciones educacionales formales vueltas a la promoción del tema, la violación ocurre en la propia política de seguridad pública. Son empleadas técnicas de investigación, sin mínimos criterios legales objetivos, banalizando distintas prácticas inadecuadas, desde la vulgar "criptoanálisis de manguera de goma"[51] hasta el sofisticado *hacking* gubernamental.[52]

En el Legislativo, entre muchas propuestas normativas,[53] la reforma del Código de Proceso Penal[54] puede regular medios para la interceptación telemática; el proyecto de ley nº 2.518/2019 puede prever un mecanismo para el rastreo activo de blancos; y la versión del proyecto de ley nº 2.630 de 2020 aprobada en el Senado crea para aplicaciones de mensajes instantáneos la obligación de "rastreabilidad de comunicaciones".[55]

En el Judiciario, cabe al Supremo Tribunal Federal apreciar la constitucionalidad del bloqueo de WhatsApp, teniendo como eje la exigibilidad de que la compañía abandone patrones cifrados de seguridad para posibilitar el acceso investigativo a datos de sus usuarios. Los votos ya proferidos en la ADPF nº 403,[56] por el ministro Edson Fachin, y en la ADI nº 5527,[57] por la ministra Rosa Weber, protegen al cifrado. El juzgado está suspendido desde mayo del 2020, sin garantías de que no será legitimada la quiebra del cifrado. Además, cabe a la Corte analizar el valor de la prueba producida durante la investigación policial mediante acceso, durante flagrantes, sin autorización judicial, a datos en teléfonos celulares, relacionados al delito y aptos a identificar el agente, conforme el Tema de Repercusión

---

51 Rodrigues, G. (2022). Acesso policial a celulares no Brasil e a banalização da "criptoanálise de mangueira de borracha". *IRIS - Instituto de Referência em Internet e Sociedade.* https://irisbh.com.br/acesso-policial-a-celulares-no-brasil-e-a-banalizacao-da-criptoanalise-de--mangueira-de-borracha/

52 Rodrigues, G. (2021). Hacking governamental e a indústria da insegurança digital. *IRIS - Instituto de Referência em Internet e Sociedade.* https://irisbh.com.br/hacking-governamental-e-a-industria-da-inseguranca-digital/ ; Amaral, P., Canto, M., Pereira, M. C. M., Ramiro, A.. (2022) Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil. *IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife.* https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/.

53 Ramiro, A., Canto, M. Real, P. C., Lima, J. P., Aguiar, T. (2020). O Mosaico Legislativo da Criptografia no Brasil: uma análise de projetos de Lei. *IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife.* https://ip.rec.br/publicacoes/o-mosaico-legislativo-da-criptografia-no--brasil-uma-analise-de-projetos-de-lei/.

54 Congresso Nacional. (s.d.) "Projeto de Lei do Senado n° 156, de 2009" (Reforma do Código de Processo Penal.). https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pls-156-2009

55 Rodrigues, G. R., Santarém, P. R. S., Vieira, V. B. R. (2022). Comunicações privadas, investigações e direitos: rastreabilidade de mensagens instantâneas. IRIS – Instituto de Referência em Internet e Sociedade. https://irisbh.com.br/publicacoes/comunicacoes-privadas-investi-gacoes-e-direitos-rastreabilidade-de-mensagens-instantaneas/

56 Supremo Tribunal Federal. (s.d.). *ADPF 403*. https://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500

57 Supremo Tribunal Federal. (s.d.) *ADI 5527*. https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282

General nº 977[58](ARE 1042075).[59]

Dicho escenario abre posibilidades de arbitrariedades en la averiguación de la vida íntima y privada y en el acceso indebido a datos de cualesquiera personas, afectando de forma especial a segmentos poblacionales más vulnerables, víctimas habituales de investigaciones represivas, sin efectivas garantías legales y constitucionales.

• Iniciativas de la sociedad civil para la defensa, mantenimiento y difusión social de un cifrado fuerte en Brasil

Frente a los desafíos, la sociedad civil ha asumido un papel activo en esa disputa. Investigadores, activistas, colectivos y organizaciones no gubernamentales han tomado la delantera de la defensa del cifrado en Brasil y alrededor del mundo. En esta sección del reporte, abordamos las acciones pautadas por la sociedad civil brasileña con el objetivo de frenar las amenazas al cifrado fuerte.

La ADPF nº 403 y la ADI nº 5527 son demostrativos de esa delantera, a pesar de que el carácter constitucional de tales acciones exigieran determinadas condiciones para figurar en el polo activo de la proposición, la sociedad civil se hizo presente en las audiencias públicas, y participó activamente del proceso como *amicus curiae*. Además de intervenciones judiciales, las diferentes frentes ocupadas por los movimientos pro-cifrado, amplían la capilaridad en espacios que van desde la difusión del papel del cifrado en las rutinas humanas, hasta el *advocacy* en políticas públicas.

Las Criptofestas son un ejemplo de las posibilidades reinventadas por la sociedad civil para articular y difundir una cultura criptográfica. Su emergencia es de alrededor del 2012, en Australia, como respuesta a la aprobación de un proyecto de Enmienda legislativa para cibercrímenes, que condicionaba la retención de los datos del usuario por dos años[60].

La propuesta de la fiesta surge con algunos principios orientadores: a) la descentralidad, la organización debe ser abierta, sin inclinaciones de poder; b) ser un espacio de cambio; de este modo la participación no debe ser condicionada a tener un conocimiento previo sobre cifrado, pero al deseo de aprender y cambiar experiencias; c) poner manos a la obra y probar, por ser un espacio de autogestión, es necesario que todos colaboren, independente de su nivel de confianza o de habilidades, la construcción es colectiva; d) independencia política y comercial, a pesar de ser un espacio político, no es sano que se vincule a partidos políticos tampoco a compañías o ONGs, pues ese envolvimiento puede reducir el respecto a los demás principios; e) las herramientas recomendadas deben ser de acceso gratuito o abierto, para evitar intervenciones económicas; f) tolerancia cero a asedios

58 Supremo Tribunal Federal. (s.d.) "Tema 977 - Aferição da licitude da prova produzida durante o inquérito policial relativa ao acesso, sem autorização judicial, a registros e informações contidos em aparelho de telefone celular, relacionados à conduta delitiva e hábeis a identi-ficar o agente do crime." (Recurso extraordinário em que se discute, à luz do art. 5º, incs. XII e LVI, da Constituição da República, a licitude da prova produzida durante o inquérito policial subsistente no acesso, sem autorização judicial, de registros e informações contidas em aparelho de telefonia celular relacionado à conduta delitiva, hábeis a identificar o agente do crime.). https://portal.stf.jus.br/jurisprudenciaRepercus-sao/verAndamentoProcesso.asp?incidente=5173898&numeroProcesso=1042075&classeProcesso=ARE&numeroTema=977

59 Supremo Tribunal Federal. (s.d.) *ARE 1042075*. https://portal.stf.jus.br/processos/detalhe.asp?incidente=5173898

60 CryptoParty. (2022). ***What is a CryptoParty?*** https://www.cryptoparty.in/#what_is_a_cryptoparty

y violencias, físicas o verbales.[61]

Por su carácter descentralizado, las Cryptofestas se difundieran por el mundo, incluso en Brasil. Es necesario registrar que, por dicho motivo, no hay de forma sistematizada datos sobre todas las fiestas ya organizadas, lo que se presenta como un desafío a la presente investigación. El sitio de la Cryptoparty[62] posee registro de 6 fiestas en Brasil, siendo: la CriptoTrem, realizada en Belo Horizonte, 2019; la CriptoRave de São Paulo, realizada a cada año; la CryptoFesta Taubaté, realizada en 2017; la CriptoFesta Recife, realizada en 2018, en la capital Pernambucana; la nanoCRYPTOFesta Tarrafa, realizada en 2018, en la ciudad de Florianópolis; y el Criptobaile, realizado en 2018, en el Distrito Federal. Es necesario destacar la existencia de otras Cryptoparty que no están correlacionadas en el sitio, como ejemplo tenemos la CriptoFunk en Rio de Janeiro,[63] la CriptoJP, en Paraíba, y la CriptoBaião en Ceará.[64]

Otra manera de articulación de la sociedad civil en Brasil es la promoción de coaliciones, frentes que reúnen distintas personas e instituciones, como la Coalición Derecho en las Redes - CDR[65], una red con más de 50 organizaciones académicas y de la sociedad civil, que pauta, entre otras cosas, la defensa de una criptografía fuerte. La CDR propuso en 2020, el lanzamiento del CriptoAgosto,[66] inspirado en otras iniciativas como el Dia de la Internet Segura, en el mes de febrero, en las articulaciones de Global Encryption Coalition, y en las mencionadas CryptoFestas. Desde entonces las organizaciones participantes de la Coalición, se han comprometido a desarrollar acciones y proyectos en el mes de agosto, que remarquen la importancia del cifrado y su defensa.

Otra agenda construida por la sociedad civil, es la articulación de una Alianza latinoamericana y caribeña por la defensa del cifrado, la AC-LAC. Creada por la unión de 23 organizaciones de distintos países de América Latina y Caribe, con la misión de producir una plataforma colectiva que amplíe el conocimiento sobre cifrado como derechos fundamental y humano, además de articular esfuerzos transnacionales para cambios y movilizaciones en defensa del cifrado, avanzando de este modo con una agenda proactiva.[67]

En ese sentido, las organizaciones de la sociedad civil brasileña asumen protagonismo en defensa de una agenda pro-cifrado, en la búsqueda de refrenar los avances de las amenazas a un cifrado fuerte.

• Conclusión

Distintas amenazas y ataques que el poder público impone a derechos humanos envolviendo el cifrado derivan, en alguna medida, de la equivocada premisa de haber una

61 CryptoParty. (2022). What is a CryptoParty? https://www.cryptoparty.in/#what_is_a_cryptoparty

62 CryptoParty. (2022). What is a CryptoParty? https://www.cryptoparty.in/#what_is_a_cryptoparty

63 CriptoFunk – criptografe dados, descriptografe o corpo. (s.d.) https://criptofunk.org/

64 Intervozes. (2020, outubro 29) Levante sua Voz: Ep #5: Criptofestas e criptografia [Video]. YouTube. https://www.youtube.com/watch?v=nHRpRfwVtLQ

65 Coalizão Direitos Na Rede. (2016). Quem somos? https://direitosnarede.org.br/quem-somos/

66 Coalizão Direitos Na Rede. (2020). CRIPTOAGOSTO: Coalizão Direitos na Rede elege o mês de agosto para discutir criptografia. https://direitosnarede.org.br/2020/08/04/criptoagosto-cdr-elege-o-mes-de-agosto-para-valorizar-a-criptografia/

67 Aliança para Criptografia na América Latina e Caribe. (202?). Sobre nós. https://ac-lac.org/pt/sobre-nos/

contraposición irreconciliable entre protección de datos digitales y seguridad pública. Desde la primera criptoguerra hasta las prácticas de *hacking* gubernamental por el gobierno brasileño, Estados de todo el mundo no parecen comprender institucionalmente la importancia del cifrado fuerte para el mismo interés público, en distintas dimensiones. Los riesgos identificados en Brasil demandan soluciones específicas y locales, pero deben ser encarados como parte de un complejo problema global, que también evoca cuidados internacionales, con la cooperación entre países.

Más allá de la libertad de expresión y de la privacidad, se limitan una serie de otros derechos fundamentales a los seres humanos cuando prácticas gubernamentales no sólo apoyan como incentivan abusos, excesos y omisiones por parte de compañías privadas que se ponen en la condición tecnológica y económica de tutoras de la ciberseguridad de gran parte de la población que utiliza los recursos de la sociedad de la información sin capacidad para evaluar personalmente la confianza del funcionamiento de sus dispositivos y sistemas y redes digitales.

Pero, conforme la reciente relatoría del Consejo de Derechos Humanos de la ONU, los repetidos esfuerzos demostrativos de beneficiarios del cifrado, de grupos vulnerables a sectores estratégicos, no se mostraron suficientes para reducir tales peligros. Además de renovar las recomendaciones para compañías y gobiernos, se hace necesaria la asunción de compromisos comunes en la comunidad internacional, para que las soluciones y los avances en la protección, defensa y promoción del cifrado fuerte se alcancen de modo consistente y armónico en todos los países.

• Recomendaciones

Desde el escenario diagnosticado, se sugieren los siguientes pasos de incidencia para las organizaciones de la sociedad civil, teniendo como objetivo la promoción, defensa y protección de los derechos humanos relacionados a la regulación del cifrado en Brasil:

• Actuar junto al Poder Legislativo para:

a.Señalar, en los proyectos de ley en general, los riesgos de iniciativas normativas que estipulen restricciones directas o indirectas, generales e indiscriminadas sobre el uso del cifrado, previendo, por ejemplo, prohibiciones, criminalización, imposición de patrones de cifrado débiles o requisitos para verificación general obligatoria del lado del cliente;

b. Señalar, en los debates del Nuevo Código de Proceso Penal y de la Ley General de Protección de Datos en Investigaciones Criminales y Seguridad Pública, que la interferencia en la encriptación de comunicaciones privadas de particulares solo deba ser efectuada cuando autorizada por órgano judiciario independiente y caso a caso, teniendo como blanco individuos si es estrictamente necesario para la investigación de crímenes graves, o para la prevención de crímenes graves, o amenazas a la seguridad pública o a la seguridad nacional;

c. Estimular una agenda positiva para promover y proteger el cifrado fuerte, por medio de debates, eventos, seminarios y audiencias públicas.

• Actuar junto al Poder Judiciario para:

a. acompañar el desarrollo de las acciones de control concentrado de constitucionalidad (ADI 5527 y ADPF 403), evaluando la oportunidad y conveniencia de solicitar audiencias en gabinete con los (as) ministros (as) do Supremo Tribunal Federal;

b. acompañar el desarrollo del ARE 1042075, evaluando la oportunidad y conveniencia de solicitar audiencia en gabinete con el ministro Relator, Dias Tóffoli, así como con los demás integrantes de la Corte;

• Actuar junto al Poder Ejecutivo para:

a. fortalecer la supervisión institucional y el monitoreo social de las actividades de contratación de *hacking* gubernamental;

b. llamar la atención de la opinión pública sobre actividades abusivas, como por ejemplo el criptoanálisis de manguera de goma;

c. estimular una agenda positiva para promover y proteger el cifrado fuerte, por medio de debates, eventos, seminarios y audiencias públicas.

d. En el ámbito de las organizaciones de la sociedad civil, promover eventos de debate sobre el asunto, envolviendo especialmente las organizaciones vinculadas a agendas como:

amici curiae na ADI 5527 y ADPF 403;

integrantes de la AC-LAC;

organizadoras de eventos de difusión, como criptofestas, criptoagosto etc.

País: Chile

Autores: Alex Renan de Sousa Galvão, Isabelle Brito Bezerra Mendes, Iago Capistrano Sá, Larissa Rocha, Letícia Alves, Luis Henrique de Menezes Acioly, Matheus Fernandes da Silva, João Araújo Monteiro Neto

Organización: Grupo de Estudos em Tecnologia, Informação e Sociedade (GETIS)

El uso del cifrado como un mecanismo de combate a la vigilancia estatal y la protección de garantías y derechos fundamentales – una evaluación socio-legal de la propuesta regulatoria chilena

• Introducción

Observando el rápido desarrollo de las tecnologías informacionales y de las telecomunicaciones es posible percibir que el tema del cifrado ha cobrado un importante rol en las discusiones y en los estudios académicos y políticos. El presente trabajo busca analizar como el cifrado ha sido abordado en Chile, mapeando como dicho tema es tratado en los más distintos sectores sociales con el objetivo de identificar indicaciones positivas de adopción de la tecnología, bien como los riesgos vinculados a ella.

Desde los años 90 estudios y políticas son producidos en Chile poniendo de relieve la temática de la ciberseguridad. El 2017, fue propuesta la Política Nacional de Ciberseguridad, con direccionamientos expresos a la impulsión del desarrollo del cifrado. A partir de ese año, Chile pasó por un proceso particular de maduración legislativa de la temática, con la creación de leyes alrededor del tema, la creciente involucración de la sociedad civil señalando la necesidad de incluir previsiones sobre cifrado en la Constitución, además del crecimiento de actividades en el campo de la ciberseguridad. Se comprende, así, ser coherente el estudio de esa realidad para el fortalecimiento de la idea de lo que ha sido producido en el contexto latinoamericano, así como para impulsar el estudio sobre la legislación del cifrado en nuestro país.

• Metodología

Desde un abordaje de investigación socio-legal orientada al estudio de caso, el trabajo propuesto explora el objeto de estudio a través del análisis bibliográfico y documental (examen de legislaciones e instrumentos normativos, noticias, publicaciones y notas técnicas legislativas, artículos periodísticos y demás instrumentos cualitativos). El principal objetivo es traer luz sobre los argumentos y racionalidades que promueven o impiden el desarrollo de

mecanismos regulatorios que establecen la adopción del cifrado como medio de protección de derechos digitales y de combate a la vigilancia digital.

• Contexto y antecedentes

Según el reporte producido por la Organización de Naciones Unidas - ONU (2022), Chile es el segundo país de América Latina más avanzado en términos de gobierno electrónico. Pero la afirmación debe ser leída con moderación ante el contexto sociopolítico vivido por el país especialmente en lo relacionado al escenario legislativo, como se discutirá más adelante. En Chile, las discusiones referentes a la ciberseguridad no son recientes, puesto que desde el año de 1999 el país impulsa estudios sobre la cuestión y, desde entonces, ya ha producido por lo menos cinco instrumentos de planificación *("Chile: Hacia la sociedad de la información"; "Agenda Digital: Te acerca al futuro"; "Estrategia Digital"; "Agenda Digital: Imagina Chile"; Agenda Digital*) que fueron base para las políticas gubernamentales e impulso de las discusiones sobre el tema.

Ya en el año de 2017 fue establecida la Política Nacional de Ciberseguridad (PNCS), con directrices a ser alcanzadas hasta finales de 2022. Entre los objetivos se señala: el desarrollo de infraestructura hecha para enfrentar incidentes de ciberseguridad; el Estado como garantizador de derechos de las personas en el ciberespacio; el desarrollo de una cultura de ciberseguridad a través de la educación y de buenas prácticas; el establecimiento de relaciones de cooperación de ciberseguridad con otros países; así como la participación activa en las discusiones internacionales.[68]

Específicamente en lo que se refiere al cifrado, la PNCS reconoce el valor de la tecnología al comprehender que esta permite el suministro de alto nivel de confidencialidad e integridad para la información, siendo una posibilidad relevante para la estrategia de seguridad externa del país. A partir de esta comprensión, establece que las medidas adoptadas deben promover la adopción de criptografía punta-a-punta para los usuarios, alineadas con los patrones internacionales, debiendo ser evitado a todo costo el uso de tecnologías inseguras.[69]

Vale decir que la motivación de esas discusiones y preocupaciones referente a la ciberseguridad, específicamente a la criptografía, está especialmente relacionada con el constante desarrollo tecnológico, los riesgos y amenazas a los derechos fundamentales de las personas y la seguridad estatal.

Como ejemplo, es mencionado el creciente interés por el espionaje digital por parte de los gobiernos de América Latina, como demuestra el reporte *Hacking Team: malware de espionaje en América Latina*, en el cual es expuesto que la mayoría de los países de la región estuvo involucrada con la *Hacking Team*, cuestionada compañía italiana creadora del Remote Control System (RCS), un software espía vendido a organizaciones gubernamentales alrededor del mundo.[70]

---

68 CHILE. (2017) Política Nacional de Ciberseguridad. [S. l.: s. n.] https://www.cnc.cl/wpcontent/up loads/2020/02/Pol%C3%ADtica-Nacional-Ciberseguridad.pdf

69 CHILE. (2017) Política Nacional de Ciberseguridad. [S. l.: s. n.] https://www.cnc.cl/wpcontent/up loads/2020/02/Pol%C3%ADtica-Nacional-Ciberseguridad.pdf

70 De Acha, G. (2016) Hacking Team: malware para la vigilancia en América Latina. Derechos Digitales https://www.apc.org/fr/node/21624

No es difícil comprender que fugas y fallas en la seguridad, en ese aspecto, son catastróficas. Consciente de eso, Chile tiene discutido la mejoría de acciones relativas a la temática, enfocando en la seguridad de la infraestructura crítica de la información. Como será desarrollado a seguir, diversos sectores sociales se han esforzado en la reglamentación del cifrado, estudios y establecimiento de patrones y buenas prácticas.

• Evaluación del panorama chileno

El crecimiento del uso y de los riesgos que implican su utilización de tecnologías de la información que pueden afectar no solamente los derechos fundamentales de las personas, sino también la seguridad del país, fomentaran el desarrollo de la Política Nacional de Ciberseguridad do Chile.

Sirve como ejemplo de esa percepción la actuación de la compañía "Hacking Team", que desarrollaba potentes *softwares* de espionaje, siendo la principal aplicabilidad de ellos la invasión de dispositivos electrónicos y bases de datos para obtener informaciones, teniendo incluso comercializado sus softwares con diversas agencias gubernamentales. La lógica por tras de los *Malwares* desarrollados es que llama atención: la "Violación intencional de sistemas informáticos para hacer cumplir la ley, tirando partido de sus grietas reglamentares".[71]

En ese contexto, Chile adquirió el sistema Galileo da Hacking Team, cuyo nombre fue modificado para Phantom, no habiendo sido la adquisición hecha de forma clara y transparente, ya que, de acuerdo con Partarrieu y Jara (2015), la compra por la policía investigativa de Chile fue hecha de forma sigilosa y descubierta después del ataque informático a la compañía proveedora del software que resultó en la divulgación de varios correos electrónicos.[72]

El uso del software del malware tiene su legalidad cuestionada, teniendo en cuenta que la interceptación de comunicaciones en los países generalmente depende de orden judicial y la tecnología del software tiene otras funcionalidades invasivas además de la interceptación, como geolocalización, activación de cameras y micrófonos.[73]

Considerando el potencial invasivo de los sistemas vendidos por Hacking Team, existe recelo de las consecuencias que la utilización de tecnologías de vigilancia puede acarrear a los derechos humanos, principalmente en lo que se vincula a la libertad de expresión y derecho a la privacidad. En Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión, ONU e a OEA (2013)[74]indicaron preocupación, teniendo en vista que algunos Estados estaban interceptando comunicaciones particulares con finalidades políticas.

---

71 De Acha, G. (2016) Hacking Team: malware para la vigilancia en América Latina. Derechos Digitales https://www.apc.org/fr/node/21624

72 Partarrieu. B y Jara. M. (2015). Los correos que alertaron sobre la compra del poderoso programa espía de la PDI. CIPER. Disponible en https://ciperchile.cl/2015/07/10/los-correos-que-alertaron-sobre-la-compra-del-poderoso-programa-espia-de-la-pdi

73 De Acha, G. (2016) Hacking Team: malware para la vigilancia en América Latina. Derechos Digitales https://www.apc.org/fr/node/21624

74 https://www.oas.org/pt/cidh/expressao/showarticle.asp?artID=926&lID=4

El cifrado, en ese contexto, sería una relevante alternativa para proteger, ya que es una tecnología direccionada a la codificación de informaciones, a las cuales tendrían su confidencialidad preservada, volviendo el contenido indisponible a las personas que no tienen acceso o no estén autorizadas a operar la decodificación.

Destacándose en el escenario latinoamericano, sobresaliendo en la preocupación en desarrollar políticas nacionales de ciberseguridad, Chile, en el ámbito legislativo, discute actualmente el Proyecto de *Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información* (Boletín Nº 14.847-06). Iniciado por iniciativa del ex-presidente de la República Sebástian Piñera, la proposición fue entregue al Senado en marzo del 2022.

A partir del análisis del mensaje de presentación del referido proyecto de ley, se infiere el ansia política que se busca alcanzar a partir de él. Se nota la preponderancia del rol de consolidación de la seguridad de la información vinculada al ejercicio de los derechos fundamentales a través de la administración pública digital, bien como de la regulación sobre el tema junto a los particulares. Se intenta realizar una "guerra al terror" cibernética, indicando medidas de prevención a ciberataques.

El mensaje con la presentación del PL contextualiza la creación de una Agencia Nacional de Ciberseguridad que coordine el tema junto al sector privado de forma permanente para garantizar la seguridad del ciberespacio, previniendo crímenes informáticos y protegiendo a la infraestructura de tráfico de información. Como muestra, se busca viabilizar la supervigilancia, estableciendo medios para el ejercicio del Poder de Policía en el ámbito digital. El mensaje enviado al Senado de Chile por la AC-LAC, Alianza para el Cifrado en América Latina y Caribe, se contrapone desde la garantía de protección del cifrado en PL.[75]

Considerando el objetivo delineado en el mensaje de encaminamiento del proyecto de ley – con expresa mención a la finalidad de supervigilancia a través de la Agencia Nacional de Ciberseguridad,[76] el texto normativo defiere a dicha institución la función de, en conjunto con agencias de inteligencia, enfrentar amenazas a la infraestructura crítica de la información e implementar acciones preventivas, sin, todavía, especificar garantías mínimas a los ciudadanos en ese contexto (art. 9, "l"). La opacidad del procedimiento investigativo y de acciones preventivas devela el riesgo de quiebra de la privacidad permanentemente. Además, la ausencia de multi-sectorialismo – con representantes de la sociedad civil, de la universidad y del sector privado – en la composición del Consejo Técnico de la Agencia Nacional de Ciberseguridad demuestra el riesgo de mala gestión de informaciones y datos personales de los ciudadanos, obtenidos en el marco de un opaco sistema preventivo al ciberterrorismo.

Se infiere que la ausencia de garantía del cifrado en PL se contrapone al creciente movimiento de la sociedad civil por protección de los derechos digitales. La autodeterminación informativa comprende la seguridad y la privacidad provistas por el cifrado, de modo que no haya obstáculos al libre desarrollo de la personalidad en el ciberespacio.

Es importante percibir que el contexto para la proposición de la regulación es un escenario político marcado por tensiones y ensayos para un intento de ruptura con el orden constitucional heredado del gobierno de Augusto Pinochet. Aunque exista una

75 https://ac-lac.org/ac-lac-pide-incluir-cifrado-en-el-proyecto-ley-marco-sobre-ciberseguridad-e-infraestructura-critica-de-la-informacion-de-chile/

76 Chile. Senado. Proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=1484706

inmanente necesidad del Estado chileno en garantizar la seguridad de la información en sus instituciones contra amenazas, ataques cibernéticos y espionaje, ante el histórico de ataques cibernéticos sufridos en tiempos recientes[77], la cuestión no se destaca de la demanda popular por un nuevo orden constitucional. El rechazo popular por la nueva Constitución Política de Chile culmina por no traer el apoyo inherente a la cuestión del cifrado con contemplación en el Proyecto de Ley.

Encaminada primeramente al Senado, la proposición fue debatida en *Comisión de Defensa Nacional* y en la *Comisión de Seguridad Pública.* En la discusión general del proyecto, el Senador Pugh Olavarría destacó la necesidad de actualización de la Política Nacional de Ciberseguridad Chilena, vigente desde el 2017, requiriendo plazo para indicaciones.

El Boletín n° 14.847-06 revela las indicaciones presentadas, que implican supresión de expresiones, incorporación de nuevos dispositivos o incluso sustituciones, todas partiendo de senadores o del presidente de la República, aprobado por el Ministerio de Hacienda, el cual presentó Informe Financiero Complementar aduciendo que las alteraciones no significarían un gasto fiscal más grande. El plazo para las indicaciones fue ampliado hasta el 22 de noviembre del 2022.

Al respecto a las disposiciones constitucionales, el reconocimiento del derecho a la privacidad, a la protección de datos personales y a la ciberseguridad estaban entre las propuestas de la iniciativa popular nº 57.970 hecha por el Centro de Estudios en Derecho Informático (CEDI) para que fueran mantenidas y avanzadas en el nuevo texto constitucional[78], demostrando la demanda de la sociedad civil para que tales derechos sean protegidos con notable evolución técnico-jurídica en relación a la previsión constante en la constitución vigente. Se destaca que, en la iniciativa, había mención al cifrado como forma de protección de la seguridad digital[79].

A pesar de que no haya sido aprobado, el texto propuesto para la nueva Constitución chilena mostró claro avance en relación a la garantía de la ciberseguridad, teniendo en vista que la propuesta anticipaba reglas relativas a la privacidad, protección de datos, seguridad informática y promoción de derechos en el ámbito digital[80]. En su art.70, la propuesta abordaba previamente el derecho a la privacidad familiar, personal y comunitaria, haciendo mención también a la inviolabilidad de las comunicaciones privadas e incluyendo los metadatos, indicando que "[...]3. *Toda documentación y comunicación privada es inviolable, incluyendo sus metadatos. La interceptación, la captura, la apertura, el registro o la revisión sólo se podrá realizar con orden judicial previa.*"[81], limitando a la vigilancia estatal en relación a los datos provenientes de interacciones y comunicaciones realizadas por medio

---

77 Barbas, J.; Sancho, C. (2018) Cibersegurança e Políticas Públicas Análise comparada dos casos chileno e português. Instituto da Defesa Nacional e Academia Nacional de Estudios Políticos y Estratégicos de Chile.

78 Universidad de Chile. (2022) CEDI presenta iniciativa popular de norma sobre el derecho a la protección de datos personales

https://derecho.uchile.cl/noticias/183976/cedi-presenta-iniciativa-popular-de-normasobre- datospersonales#:~:text=La%20propuesta%20 del% 20CEDI%20reconoce,protegi%C3% B3% 20los%20papeles%2C%20los%20efectos

79 Universidad de Chile. (2022) CEDI presenta iniciativa popular de norma sobre el derecho a la protección de datos personales

https://derecho.uchile.cl/noticias/183976/cedi-presenta-iniciativa-popular-de-normasobre- datospersonales#:~:text=La%20propuesta%20 del% 20CEDI%20reconoce,protegi%C3% B3% 20los%20papeles%2C%20los%20efectos

80 Venturini, J. (2022) Nuevos rumbos constitucionales hacia el fortalecimiento de la privacidad y la protección de datos personales. DERECHOS DIGITALES https://www.derechosdigitales.org/19107/nuevos-rumbosconstitucionales-hacia-el-fortalecimiento-de-la-privaci-dad-y-la-proteccion-dedatospersonales/

81 Chile (2022) Propuesta Constituición Política de La República de Chile https://www.chileconvencion.cl/wp-content/uploads/2022/07/Texto-DefinitivoCPR2022-Tapas.pdf.

de dispositivos digitales[82], promoviendo de este modo la preservación de derechos de los ciudadanos, así como la continuidad del orden jurídico.

• Conclusión

A partir de la investigación emprendida es posible comprender el grado de complejidad de la cuestión envolviendo el cifrado en Chile, puesto que es latente la discusión sobre derechos digitales en ese país. Se entiende que, bajo el punto de vista legal, la tramitación del Proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información demuestra la importancia del tema en el contexto chileno, en tanto demostrada la ambición legislativa en reglamentación del traslado seguro de informaciones. La propuesta legislativa, sin embargo, demuestra el riesgo de violación al derecho fundamental de privacidad, a la medida en que permite una supervigilancia estatal en el marco del combate a los cibercrímenes, sin el contrapeso de garantías mínimas al ciudadano.

La posibilidad de interferencia de comunicaciones privadas, aliada a la obligatoriedad de compañías privadas de compartir informaciones sobre sus usuarios con la Agencia Nacional de Ciberseguridad representa, en otras palabras, la posibilidad de establecimiento de un estado de supervigilancia permanente, viabilizando dicha finalidad expresa en el mensaje de encaminamiento del PL. La centralización de la coordinación de fiscalía y normatización en términos de ciberseguridad prefigura la centralización de un poder ilimitado, en detrimento de la inviolabilidad de la comunicación. La propuesta legislativa legítima todavía el uso preventivo de acciones, en coordinación con agencias de inteligencia, sin cualquier contrapeso de protección a la privacidad del ciudadano.

El cifrado surge como instrumento de garantía de privacidad digital, resguardando el libre desarrollo de los usuarios de plataformas digitales. Con efecto, se nota la actuación de los movimientos de la sociedad civil para que se haga constar la protección del cifrado en el cuerpo textual de la propuesta legislativa. El prisma social también pudo ser observado desde la organización de la sociedad civil dada por ocasión de la Propuesta de Constitución Política da República de Chile, que, a pesar de haber sido rechazada por voto popular, muestra una sistémica y compleja organización socio-legal en pro de la garantía de privacidad, de la inviolabilidad de la comunicación, la protección de datos y demás derechos digitales. El avance de la protección constitucional de la inviolabilidad de la comunicación, y consecuentemente del cifrado, restringiría el alcance de la implementación del sistema de cibervigilancia por intermedio de una Ley sobre Ciberseguridad en el contexto chileno.

El establecimiento de garantía al cifrado en el contexto de la ciberseguridad nacional, caso no avance a nivel legal, en el texto del referido Proyecto de Ley, tendría sostén en nueva fase de la Política Nacional de Ciberseguridad, calcada en la premisa constitucional de protección de datos y sigilo de las comunicaciones, reglamentando la acción de la Agencia Nacional de Ciberseguridad chilena.

La discusión política alrededor de la malla normativa del cifrado en el referido proyecto legislativo se relaciona directamente con el avance social de protección de los derechos

82 Venturini, J. (2022) Nuevos rumbos constitucionales hacia el fortalecimiento de la privacidad y la protección de datos personales. DERECHOS DIGITALES https://www.derechosdigitales.org/19107/nuevos-rumbosconstitucionales-hacia-el-fortalecimiento-de-la-privaci-dad-y-la-proteccion-dedatospersonales/

digitales en Chile, siendo instrumento de medida del grado de maduración política en el tema, sirviendo de base para el alcance de nuevas dimensiones de derechos fundamentales.

• Recomendaciones

Una vez observado el contexto de la reglamentación del cifrado en Chile indicamos:

- Expandir la colaboración realizada por AC-LAC con otras asociaciones civiles, extendiéndose a entidades académicas nacionales y latinoamericanas para alcance de este objetivo;

- Crear una campaña de concientización masificada de la comunicación, con el objetivo de alertar a la población civil chilena sobre la importancia del cifrado en el contexto de las comunicaciones y en la protección de derechos humanos digitales;

- Fomentar el compromiso y apoyo de la población a la demanda por inclusión del Cifrado en el Proyecto de Ley- Cuadro de Ciberseguridad de Chile, por medio de la movilización pública, incluso digital, fortaleciendo la negociación con miembros de las comisiones del Senado en que se tramita el proyecto de ley con ese objetivo;

- Producir conocimiento científico y académico sobre el tema por medio de la cual se presentará una visión holística sobre los impactos sociales del cifrado, incluso bajo el enfoque de ciencias sociales y trato de datos estadísticos;

- Establecimiento de un panorama concreto de viabilidad de derechos digitales, correlacionando la aplicación e interpretación de la actual Constitución a la protección del cifrado, a través de enmiendas y demás mecanismos legales, dándole bases a la eventual discusión de derechos digitales que deben constar en la próxima Constitución Política de Chile;

- Establecer medios de negociación con miembros del Poder Ejecutivo para viabilizar la implementación del cifrado en la reglamentación de la actividad investigativa y preventiva de la Agencia Nacional de Ciberseguridad chilena, a través de nueva fase de la Política Nacional de Ciberseguridad;

- Establecer un panorama de luchas legales estratégicas en pro del cifrado en el marco de una alianza de entidades de la sociedad civil de carácter nacional en Chile, buscando su garantía como derecho fundamental por reconocimiento judicial.

País: Colombia

Autor: Alejandro Moreno Baquero

Informe del estado actual de regulación de herramientas de encriptación en Colombia y posibles acciones de mejora

• Introducción

En este informe se presentará el estado actual en Colombia de políticas públicas e iniciativas no gubernamentales en relación con el uso, prohibiciones y derechos relacionados con las tecnologías de cifrado o encriptación. Así mismo, se hará un recuento de los principales desafíos y discusiones en el entorno colombiano en relación con la regulación de dichas tecnologías, incluyendo las posibles oportunidades de mejora identificadas.

El principal objetivo del presente informe es señalar las posibles ambigüedades que pueden existir en Colombia en materia normativa en relación con el uso de las tecnologías de cifrado. Como se elaborará en este informe, se expondrá como tal falta de claridad puede deberse principalmente de cuerpos normativos que resultan anacrónicos y no responden a de forma suficiente a necesidades actuales, especialmente en relación con la protección a grupos en condición de vulnerabilidad, tales como actores de la sociedad civil, defensores de derechos humanos, activistas o periodistas.

• Metodología

Como metodología del presente informe se planteó una consulta de fuentes normativas, académicas, iniciativas privadas y públicas, notas periodísticas, procesos judiciales y administrativos, así como otras fuentes bibliográficas de diversa índole, que pudiesen referirse directamente a la regulación de tecnologías de encriptación y sus efectos en Colombia.

Posteriormente, producto de esa revisión, se contrastaron las diferentes fuentes entre sí, para determinar los puntos en que los desarrollos normativos vigentes en materia de encriptación se encuentran desarticulados o resultan insuficientes para efectos de garantizar los derechos de los ciudadanos, especialmente como resultado del avance tecnológico experimentado en las últimas décadas. Dicho análisis se realizó, presentando especial atención a la utilidad que representa el uso de las tecnologías de cifrado para la protección de grupos en condición de vulnerabilidad en espacios digitales, tales como defensores de derechos humanos, activistas, periodistas, entre otros.

Así mismo, el presente informe cuenta con la retroalimentación de la Fundación Karisma, una de las principales organizaciones de la sociedad civil que trabaja en Colombia por la defensa de Derechos Humanos en entornos digitales.[83]

83 Para conocer más sobre las iniciativas de esta organización, puede consultar: [https://web.karisma.org.co/]

Como comentario del autor a la ejecución de la metodología propuesta se destaca que, tal como se desarrollará con mayor profundidad en el cuerpo del presente informe, los principales desafíos encontrados surgieron, precisamente, del estado ambiguo y el poco desarrollo que existe respecto a cuerpos normativos o iniciativas estatales que se refieren a las tecnologías de cifrado en Colombia, que parecieran contradecirse entre sí. Así mismo, debido a que la época en que se emitieron algunas de estas normas (por ejemplo, la Ley 104 de 1993) corresponde a un contexto muy alejado del actual, especialmente en materia del uso de dispositivos electrónicos.

• Antecedentes de la encriptación en Colombia: normas de un milenio diferente

En Colombia, el primer momento en que a encriptación fue referido en un cuerpo normativo se remonta a la década de los 90's, un periodo de desarrollo importante para las telecomunicaciones en el país. Durante dicho periodo, de forma simultánea, Colombia estaba inmersa en una época violenta derivada del conflicto armado interno (cuyos efectos persisten) entre el gobierno nacional y grupos armados tales como las guerrillas de las FARC-EP, el ELN, las disidencias del M-19, paramilitares, carteles de narcotráfico y delincuencia común.

Durante dicha época, paralelamente al conflicto interno, se estaban dando los primeros pasos en el desarrollo en las redes de Internet y las comunicaciones por teléfono y radio eran un elemento usado por los diferentes actores del conflicto interno para sus operaciones. En consecuencia, como parte de la estrategia para limitar la operación de grupos armados ilegales, la Ley 104 de 1993[84] incluyó una restricción al envío de telecomunicaciones encriptadas, de la siguiente forma:

> "*Articulo 105. los suscriptores, licenciatarios o las personas autorizadas para emplear los sistemas de radiocomunicaciones [...], tendrán las siguientes obligaciones: [...] 4. No enviar mensajes cifrados o en lenguaje ininteligible*."

No debe perderse de vista entonces, para efectos de este informe, que el contexto en que se expidió la Ley 104 de 1993 respondía a dinámicas propias de ese momento, en que las comunicaciones lucían y funcionaban de forma muy diferente a como lo hacen hoy en día. En dicha época no existía la telefonía celular (introducida al país en 1994) ni el servicio de Internet a hogares, mucho menos los servicios de mensajería instantánea y otras tecnologías similares.

En contraste, hoy en día, en Colombia se ha seguido la tendencia global de masificación y popularización de servicios de telecomunicaciones, incluyendo servicios mensajería instantánea (tales como WhatsApp, Telegram o Signal) que en su gran mayoría se sirven del cifrado para garantizar la seguridad y privacidad en las telecomunicaciones.[85] Con la llegada del nuevo milenio, la masificación de las tecnologías de telecomunicaciones y de la Internet supondría una revisión a la limitación incluida en la Ley 104 de 1993, sin embargo, como se explicará más adelante, tal actualización sigue pendiente.

---

84 Cuyo objetivo era "consagra[r] instrumentos para la búsqueda de la convivencia, la eficacia de la justicia."

85 Al respecto, se invita a consultar el resultado del proyecto "El rol de los servicios OTT en el sector de las comunicaciones en Colombia 2020-2021" de la Comisión de Regulación de Comunicaciones (CRC), disponible en el siguiente enlace.

• Encriptación en Colombia: anacronismo y ambigüedades

• Desarrollos normativos

La Ley 104 de 1993, que incluyó la prohibición de envío de mensajes cifrados para "*suscriptores, licenciatarios o las personas autorizadas para emplear los sistemas de radiocomunicaciones*" tenía una vigencia original de 2 años, no obstante, ha sido renovada periódicamente.[86] Sin embargo, en sus trámites legislativos, ninguna de las leyes por medio de las cuales se ha renovado esta limitación al uso de tecnologías de cifrado ha sido sometida a un debate real o a una revisión a la luz del cambio de paradigmas sociales en relación con el uso de estas tecnologías, lo que generó una disociación entre la regulación y la realidad, que perdura hasta hoy.

En cambio, los pocos ajustes a la limitación de 1993 han desatendido las problemáticas de fondo y se han ocupado, por el contrario, de ampliar la ambigüedad de esta norma. Por ejemplo, el texto original de la Ley 418 de 1997 extendía la prohibición a personas autorizadas para emplear los *sistemas de radiocomunicaciones* entendidos como "buscapersonas [...] radioteléfonos portátiles, handys y equipos de radio telefonía móvil". En cambio, mediante la Ley 782 de 2002 reemplazó la expresión *sistemas de radiocomunicaciones* a "*todos los equipos de comunicaciones que utilizan el espectro electromagnético*" y ese es el texto que ha sido replicado subsecuentemente. El nuevo texto en todo caso, al resultar más amplio, es menos claro, toda vez que cada vez más equipos usan el espectro electromagnético de formas y contextos distintos entre sí.

En diciembre de 2022 se expidió la Ley 2272, por medio de la cual se renovó por cuatro años más la prohibición de la Ley 418 de 1997, sin que se haya actualizado esta norma, ya sea eliminando la prohibición o, cuando menos, aclarado su alcance. Se pierde de esa forma una vez más, la oportunidad para eliminar o, al menos delimitar, una restricción tan ambigua que, además, resulta anacrónica.

Adicionalmente a la Ley 418 de 1997, otra Ley que se refiere al cifrado es la ley de inteligencia y contrainteligencia colombiana (Ley 1621 de 2013). Según dicha norma, los operadores de servicios de telecomunicaciones deberán ofrecer servicios de llamadas de voz encriptadas, de forma exclusiva, a organismos que llevan a cabo actividades de inteligencia y contrainteligencia y al alto gobierno. Aun cuando esta norma es una obligación dirigida a operadores de servicios de telecomunicaciones, considero que ésta podría interpretarse como una limitación tácita en contra de la población del acceso a este tipo de servicios, ofrecidos por los operadores.

86 Primero, la Ley 241 de 1995 extendió la vigencia de la Ley 104 de 1993 por 2 años. Posteriormente, la Ley que la derogó y reemplazó, Ley 418 de 1997, reintrodujo la misma prohibición mencionada. A partir de ese momento, la vigencia de la Ley 418 de 1997 ha sido renovada por las leyes 548 de 1999, 782 de 2002, 1106 de 2006, 1421 de 2010, 1738 de 2014, 1941 de 2018.

• Pronunciamientos judiciales y administrativos

En el ámbito de control judicial, la Corte Constitucional revisó las disposiciones de la Ley 104 de 1993 que originalmente introdujeron la limitación al uso de tecnologías de cifrado. Sin embargo, la Corte[87] en 1995 consideró en ese momento que dichas restricciones eran compatibles con la recién expedida Constitución Política de 1991, en relación con la libertad de expresión (art. 20) y la privacidad (art.15). Según la Corte de aquella época, en tanto el espectro electromagnético es un bien público, los legisladores pueden regular lo que puede entenderse como su uso correcto, por lo que no excedía las facultades del legislador.

Adicionalmente, la Corte argumentó que la norma acusada no era contraria a la Constitución en la medida que la interceptación de comunicaciones debería siempre estar antecedida por una orden judicial, por lo que la limitación a tecnologías de cifrado no implicaba un acceso indiscriminado a las comunicaciones de los ciudadanos. Tal como veremos adelante, este argumento en particular no ha superado la prueba del tiempo.

Del mismo modo, la Corte sostuvo que, si una persona "nada tiene que ocultar" debería poder entonces usar siempre expresiones usadas por *toda* la sociedad.[88] Dicho análisis, sin embargo, no tuvo en cuenta los eventos en que una persona buscase ejercer su derecho a la vida íntima, incluso frente al Estado o aquellos eventos en que, por tratarse de una población objeto de vulneraciones sistemáticas, requieran mantener altos estándares de privacidad en sus comunicaciones, como ocurre con los miembros de organizaciones defensoras de derechos humanos, ambientales o periodistas.

De hecho, existen múltiples eventos en las últimas décadas y sobre todo en años recientes, que demuestran cómo los argumentos de la Corte de 1995 no se sostendrían de cara a la prueba del tiempo.[89] Eventos como interceptaciones ilegítimas a comunicaciones privadas por parte de entes investigativos del Estado, tal como el caso de las llamadas "chuzadas" del "Departamento Administrativo de Seguridad[90] y fenómenos denunciados en publicaciones tales como el Informe Especial "Un estado en la sombra: vigilancia y orden público en Colombia" emitido por Privacy International[91] son evidencias de que la vigilancia del Estado no protege de forma suficiente los derechos a la intimidad y libertad de expresión de los ciudadanos.

Sin embargo, resulta interesante contrastar el trato que le dio la Corte Constitucional en 1995 a la tecnología de cifrado con otros fallos más recientes, tales como la sentencia SU-420/19,[92] fallo hito en materia de libertad de expresión emitido por la misma Corte. En este fallo, la Corte se refirió de forma positiva al uso de tecnologías de cifrado por parte de la población, estableciendo que este tipo de tecnologías guardan estrecha relación con la

---

87 Sentencia C-586/95. Magistrados Ponentes: Dr. Eduardo Cifuentes Muñoz y Dr. José Gregorio Hernández Galindo.

88 Lo que, por demás, resulta en una visión muy reduccionista del uso del lenguaje "común".

89 Vale la pena mencionar que los siguientes magistrados discreparon, mediante un salvamento de voto, con los argumentos propuestos en el texto que fue aprobado de la sentencia: Antonio Barrera Carbonell, Eduardo Cifuentes Muñoz, Carlos Gaviria Diaz Y Alejandro Martínez Caballero. En cambio, estos Magistrados consideraron que la prohibición era contraria a la libertad de expresión y a la privacidad, por lo que debía ser declarada inexequible.

90 Al respecto, se puede consultar más detalles de este caso en: [https://www.eltiempo.com/multimedia/especiales/condena-chuzadas-del-dasmaria-del-pilar-hurtado-y-bernardo-moreno/15661480/1/index.html] y [https://www.semana.com/nacion/articulo/las-chuzadas/111197-3/]

91 Al respecto, el Informe especial puede ser consultado en el siguiente enlace: [https://privacyinternational.org/sites/default/files/2017-12/ShadowState_Espanol.pdf]

92 Sentencia SU-420/19. Magistrado Ponente: José Fernando Reyes Cuartas.

posibilidad de un individuo de expresarse de forma anónima en Internet y, por lo tanto, son tecnologías que deben ser protegidas. Según la posición de la Corte de 2019, el anonimato es un elemento esencial del derecho a la libertad de expresión.

Según explicó la Corte, el anonimato responde a la necesidad de contrarrestar la invasión que realizan compañías o gobiernos en la Internet, sobre la información y privacidad de los usuarios. En consecuencia, las tecnologías que permiten la expresión anónima de los ciudadanos en Internet, conforme a la Corte, deben protegerse. En ese sentido, se crea ambigüedad sobre el estado actual de la regulación en materia de encriptación, puesto que el razonamiento más reciente de la Corte Constitucional cambia su posición previa en la materia, aun cuando ambos fallos se encuentran vigentes.

Por otro lado, algunas entidades administrativas han adoptado de forma tácita una posición similar a la versión garantista del fallo más reciente de la Corte Constitucional. Aun cuando no se han pronunciado directamente sobre la legalidad o papel que ejerce el cifrado en la sociedad y las telecomunicaciones en contraste a la prohibición de la Ley 418 de 1997, sí han visto de forma favorable el empleo de este tipo de tecnologías. Ejemplos de estos casos pueden ser los siguientes:

Decisiones administrativas por parte de la delegatura de protección de datos personales de la Superintendencia de Industria y Comercio (SIC) en los que se cuestiona a empresas privadas por no haber implementado adecuadamente tecnologías de cifrado.[93]

Las Circulares 007 y 008 de la Superintendencia Financiera de Colombia mediante la cual se les exige a entidades vigiladas la implementación de tecnologías de cifrado para garantizar protección de la información de los consumidores financieros.[94]

La adopción de manuales de encriptación por parte de entidades estatales, como el Ministerio de Educación Nacional,[95] o la implementación de medidas de cifrado como parte de sus políticas de seguridad de información, como el Ministerio de Tecnologías de Información y Comunicaciones,[96] Ministerio de Salud y Seguridad Social,[97] o la Policía Nacional[98].

En ese sentido, aun cuando no ha habido un pronunciamiento que explícitamente modifique o suprima las restricciones incluidas en la Ley 418 de 1997, tanto las autoridades administrativas como la misma Corte Constitucional han promovido el uso de tecnologías de cifrado por parte de ciudadanos y entidades, inclusive, al punto de exigirlos en algunos casos para efectos de proteger la información contenida en los mensajes.

No obstante, la ambivalencia de las posiciones que surge, genera inseguridad jurídica y un doble estándar, especialmente perjudicial para los ciudadanos, en la medida que no resulta completamente claro si el uso de tecnologías de cifrado es considerado legal. Ese fenómeno es especialmente perjudicial en Colombia, que actualmente atraviesa una crisis

93 Resolución 32129 de 2022, disponible en: [https://www.sic.gov.co/sites/default/files/files/2022/22-161208%20VU.pdf]

94 Disponibles en: [https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/10097769/f/0/c/00]

95 Disponibles en: [https://www.mineducacion.gov.co/1759/articles-407695_galeria_07.pdf]

96 Disponibles en: [https://www.mintic.gov.co/portal/715/articles-2627_resolucion_0448_2022.pdf]

97 Disponibles en: [https://www.minsalud.gov.co/Ministerio/Institucional/Procesos%20y%20procedimientos/ASIM04.pdf]

98 https://www.policia.gov.co/sites/default/files/manual_sgsi_ponal.pdf

de vulneración de derechos y asesinatos sistemáticos de líderes ambientales y sociales,[99] quienes se beneficiarían de la tranquilidad de contar con comunicaciones seguras asistidas por sistemas de encriptación.

Otro grupo que se ve especialmente afectado en Colombia por la poca claridad y la falta de promoción de las tecnologías de cifrado es el de los periodistas. Al respecto, precisamente por la labor periodística realizada por medios de comunicación periodísticos[100] se han hecho públicos perfilamientos ilegítimos y seguimiento a profesionales dedicados al cubrimiento de noticias. En ese sentido, es claro que el aprovechamiento de tecnologías de encriptación por parte de un grupo cuyos derechos no han sido garantizados, es una pieza clave para aumentar la seguridad de la información y privacidad de estos grupos para evitar los abusos que fueron cometidos en su contra.

Respecto a la incidencia de las decisiones judiciales, es importante traer a colación que, en 2017, el entonces Fiscal General de la Nación sugirió (en un debate análogo al que ocurrió en Brasil) que se facultara a los jueces colombianos para ordenar que en algunos casos de investigaciones criminales se pudiera ordenar la reversión del cifrado. A pesar de que esta propuesta no tuvo tracción y, por lo tanto, no fue llevada a un proceso legislativo o administrativo para ser implementada, es un antecedente sobre la posición que mantienen algunos sectores de la sociedad que, en potencia, puede generar riesgo sobre el ejercicio de derechos fundamentales como la privacidad o la libertad de expresión.[101]

• Iniciativas no gubernamentales

En 2015, la Fundación Karisma ya había advertido el estado ambiguo en que se encuentra la regulación respecto a la encriptación. En su informe presentado al El Relator Especial para la promoción y protección de la libertad de opinión y expresión de las Naciones Unidas, David Kaye[102], Karisma ya había denunciado la ambigüedad y anacronismo que actualmente afectan la *regulación* de la encriptación en Colombia, así como los riesgos asociados a estas dificultades.

De igual forma, la Fundación Karisma, en conjunto con la Fundación para la Libertad de Prensa (FLIP) y otras organizaciones no gubernamentales publicaron el "Manual Antiespías: *Herramientas para la protección digital de periodistas*"[103]. En el Manual, una de las recomendaciones que se incluyen de forma reiterada es la utilización de tecnologías de encriptación en las comunicaciones de periodistas de forma que se disminuya el riesgo de

---

99 AL respecto, se recomienda consultar los informes realizados por Global Witness, que ubica a Colombia como el país con mayor asesinato de líderes ambientales disponible en: [https://www.globalwitness.org/es/last-line-defence-es/] y las cifras publicadas por el Instituto de Estudios para el Desarrollo y la Paz -INDEPAZ- en su Radiografía de la violencia contra los líderes asesinados en Colombia, disponible en [https://indepaz.org.co/wp-content/uploads/2021/09/L%C3%ADderes-ambientales-asesinados-desde-la-firma-del-acuerdo.pdf]. De igual for-ma, la Defensoría del Pueblo ha revelado las alarmantes cifras de asesinatos a líderes sociales en Colombia, al respecto, se recomienda consultar: [https://www.defensoria.gov.co/-/en-los-primeros-8-meses-del-a%C3%B1o-se-han-presentado-136-homicidios-contra-l%C3%ADderes-socia-les-y-personas-defensoras-de-dd.-hh.] Estas son algunas de muchas evidencias sobre la crisis que actualmente atraviesa el país en relación con la seguridad de líderes sociales y ambientales.

100 Al respecto, el medio de comunicación Semana hizo pública la siguiente nota periodística: [https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpetas-secretas-investigacion-semana/667616/]. De forma similar, El Mundo publicó el siguiente reportaje: [http://www.elmundo.com/noticia/-Perfilamientode-periodistas-compromete-al-Ejercito-colombiano/379739].

101 Disponible en el siguiente enlace: [https://www.elespectador.com/tecnologia/romper-el-cifrado-de-whatsapp-una-mala-idea-article-687353/]

102 Disponible en: [https://web.karisma.org.co/cifrado-de-comunicaciones-y-anonimato-en-colombia-comentarios-presentados-al-relator-especial-david-kaye/]

103 Disponible en: [https://www.flip.org.co/images/Documentos/manual-antiespias.pdf]

afectación a la privacidad y otros derechos fundamentales en casos de interceptación de comunicaciones.

A pesar de estas iniciativas, el tema no ha ganado la atención que requiere en Colombia y la ambigüedad normativa en materia de encriptación no ha tenido la atención que merece de parte de más actores no gubernamentales tales como organizaciones de la sociedad civil o académicos.

• Conclusión

En conclusión, en Colombia sigue sin ser claro qué comunicaciones pueden cifrarse y ni el alcance que puede tener el monitoreo del espectro electromagnético sin considerarse interceptación de comunicaciones ilegítimas.

El marco ambiguo y anacrónico de la regulación en materia de encriptación en Colombia tiene efectos negativos en dos dimensiones. Por un lado, pareciera imponerse una carga injustificada sobre la sociedad, pues restringe el uso de una tecnología que, tal como describió la Corte Constitucional en el fallo SU-420/19, facilita la materialización de los derechos fundamentales de libertad de expresión e intimidad. En segunda medida, porque se desaprovecha las oportunidades de incentivar el uso de tecnologías de cifrado orientado a grupos en condiciones de vulnerabilidad tales como defensores de derechos humanos, activistas ambientales y de otras causas, así como periodistas.

En Colombia es común la expresión popular “el que nada debe, nada teme” como una excusa para exhortar a alguien a divulgar información privada. Ese es el raciocinio que llevó a la expedición de la Ley 104 de 1993 y sustenta la Sentencia C-586/95 (que se recuerda, fue aprobada en una mayoría de 5 a 4). No obstante, es un argumento que no es lógico en el panorama actual pues la experiencia de abusos sistemáticos a los derechos de los ciudadanos por parte del gobierno y de actores ilegales, ampliamente documentados, evidencia que se deben exigir estándares de privacidad suficientes, por ejemplo, a través de la legitimación y promoción de tecnologías de encriptación pues resulta necesario para garantizar derechos fundamentales frente a los desequilibrios de poder existentes.

De forma similar a como le ocurre a una persona cuando su computador o celular le avisa que debe actualizar su sistema operativo, al Estado colombiano le ha llegado una notificación en letras rojas sobre la necesidad de revisar el estado actual de las políticas públicas en materia de encriptación y cifrado.

• Recomendaciones

• Como recomendaciones, para efectos de la promoción de las tecnologías de encriptación para los miembros de la sociedad, de forma que se aprovechen los beneficios de las mismas, se debería:

• Por parte del gobierno, abrir el debate sobre las modificaciones que requiere la regulación vigente en materia de cifrado y su acceso por parte de los ciudadanos.

• Por parte del gobierno, adicionalmente, debe desarrollar políticas que promuevan el uso de tecnologías de encriptación, en favor de toda la sociedad y especialmente, de grupos en riesgo de vulneración de sus derechos.

• Por parte de otros sectores, tales como la academia o la sociedad civil, existe un llamado para promover el debate y el seguimiento a los efectos que tiene la situación actual de regulación de las tecnologías de cifrado para efectos de producir soluciones y recomendaciones puntuales.

• Por parte de la sociedad, debe promoverse el uso adecuado de tecnologías de cifrado como una (de muchas) medidas necesarias para garantizar materialmente derechos fundamentales como la privacidad o la libre expresión.

• En general, como sociedad, Colombia debe realizar un llamado a las autoridades, que les presione a implementar políticas públicas articuladas en materia de cifrado y en general, en el uso de tecnologías cuyo impacto pueda limitar o beneficiar la protección de derechos fundamentales.

Países: El Salvador, Cuba, Nicaragua y Panamá

Autores: Abdías Zambrano y Lia Hernández

Organización: IPANDETEC

Panorama general del cifrado en Centroamérica

• Introducción

La constante búsqueda de soluciones de seguridad de la información para la protección de los datos personales, ha popularizado el uso de la criptografía o encriptado. A pesar de esto, la región centroamericana y caribeña hispanohablante en general no regula el encriptado en ninguna de sus normas legales a pesar del uso extendido de aplicaciones y plataformas que utilizan este tipo de tecnología. Sin embargo, El Salvador y Cuba son la excepción a la regla.

En ambos países podremos encontrar de manera general regulaciones de distinta índole. Este artículo considera los derechos que se protegen en ambos países mediante el encriptado, la regulación vigente sobre esta tecnología analizando el estado de derecho, y el uso actual que le da la población de ambos países en vista de las restricciones vigentes, en contraste con sus culturas de privacidad.

Igualmente analizaremos la situación de algunos países de la región, considerando su regulación actual conexa en materia de telecomunicaciones y privacidad de los datos. El informe también analiza la situación política actual para comprender el contexto de las iniciativas legislativas.

• Metodología

La metodología utilizada para el presente escrito es completamente exploratoria y cualitativa. La región no presenta estudios o análisis profundos de su regulación del encriptado que pudieran ser contrastados en esta investigación por lo que creemos que este puede ser un aporte para la comunidad académica y de sociedad civil interesada en los derechos que giran en torno de la criptografía. Al ser meramente información textual se analizaron cualitativamente los contenidos que se encuentran debidamente referenciados en este informe. También se utilizó un mapa comparativo global del encriptado que permite conocer su estado a nivel internacional.

Es precisamente la falta de información el principal obstáculo encontrado para el informe. En los casos de Cuba y Nicaragua, la falta de digitalización de los textos legales y del férreo control de la libertad de expresión lo que dificulta encontrar críticas objetivas a sus regulaciones provenientes de voces disidentes u opositoras, así como de académicos

y gremios legales en contra. Toda la información referenciada y analizada puede ser encontrada en Internet.

Por otro lado, comprender el encriptado en cada país analizado es realizar un análisis del desarrollo histórico legal y cultural del derecho de privacidad y de otros derechos desarrollados durante los últimos años.

• Contexto y antecedentes

El cifrado es una tecnología que no deja de ser muy discutida. Algunas personas creen que su existencia sin 'backdoors' o puertas traseras permite el tráfico de personas, terrorismo, pornografía infantil u otros delitos. Sin embargo, la existencia de esa puerta puede ser utilizada por otros actores, no necesariamente gubernamentales. El cifrado es justamente lo contrario, es un garante de la democracia y de las libertades de los ciudadanos.

Dentro de los países analizados, encontramos países con una cultura política abocada a la izquierda como lo es el caso de Nicaragua y Cuba. En el caso de ambos países se les acusa de mantener gobiernos ilegítimos, en el caso de Cuba a través de un golpe de Estado, mientras que Nicaragua inicia con un proceso democrático que ha sido desvirtuado con elecciones ilegítimas y sin transparencia durante los últimos años.

En el caso de Cuba es una isla del caribe hispanohablante. En el país se mantiene una dictadura con más de cincuenta años de funcionamiento, considerada por algunos estudiosos una democracia popular, con tintes socialistas y comunistas. El régimen cubano ha sido ampliamente criticado por organismos internacionales y organizaciones de la sociedad civil por las constantes violaciones a los derechos humanos. Durante 2021 y 2022, masivas protestas contra el gobierno han sido cruelmente reprimidas por los estamentos de seguridad. El país ha sido declarado por la organización internacional Freedom House como una nación donde no existen libertades en línea y en espacios físicos en sus más recientes reportes anuales.

Por otro lado, Nicaragua es un país perteneciente al subcontinente centroamericano. Desde 1985, de forma interrumpida, ha sido gobernada por Daniel Ortega, y desde 2017 por su esposa como fórmula vicepresidencial. Para algunas personas, su forma de gobierno es un gobierno presidencialista, pero para otros es considerada una dictadura por recibir constantes críticas sobre su respeto a los derechos humanos, la legitimidad de los procesos democráticos, y la supuesta violación a las leyes vigentes y la Constitución sobre la reelección en el país. Al igual que Cuba, se puede observar un constante deterioro de las garantías en espacios físicos y digitales. Freedom House considera que es parcialmente libre en internet, mientras que es considerado sin libertades en su informe global de libertades. Al mismo tiempo se considera que el gobierno espía las comunicaciones de ciudadanos, opositores, religiosos, políticos, entre otros.[104]

A pesar de ser naciones relativamente cercanas geográficamente hablando, El Salvador y Panamá mantienen grandes diferencias en su estado de derecho y forma de gobierno respecto a Nicaragua y Cuba. El caso de El Salvador, es una república presidencialista anclada en el centro de América. Durante unos cuarenta años mantuvo gobiernos autoritarios que

104 Bow, J.C. (2018). Ortega espía con tecnología israelí. *Confidencial*. https://www.confidencial.digital/politica/ortega-espia-con-tecnologia-israeli/

terminaron en una guerra civil. Después de la vuelta a democracia, recientemente se le acusa por diversos organismos internacionales de mantener un gobierno con tintes autoritarios que no respeta la separación de poderes. De igual forma se le acusa de no respetar derechos humanos y garantías fundamentales. Ejemplo de esto es el uso del sistema Pegasus para vigilar activistas de derecho humanos, políticos y periodistas de un medio de comunicación impreso crítico del gobierno.[105]

Finalmente, Panamá es una democracia presidencialista. El país centroamericano, posterior a una dictadura, ha mantenido gobiernos elegidos democráticamente durante los últimos treinta años y es considerado un país con libertades aseguradas. Al igual que El Salvador, el gobierno de este país adquirió el sistema Pegasus y posteriormente se abrieron diversas investigaciones y procesos judiciales por espionaje y violación a la privacidad de las comunicaciones de los ciudadanos.[106]

Todos los países examinados se rigen por el derecho continental y mantienen en su ordenamiento jurídico, desde sus cartas magnas hasta decretos y leyes, normas sobre privacidad y seguridad de las comunicaciones.

• Contexto actual del cifrado en Centroamérica

En las subregiones de Centroamérica y el Caribe no encontramos normas generales de encriptado, sin embargo, sí encontramos menciones explícitas sobre esta tecnología. En el caso de El Salvador, no existe una ley que regule su utilización o en su defecto la prohíba, sin embargo, en materia procesal y de telecomunicaciones, se obliga a los operadores de telefonía a asegurar a las autoridades la decodificación de las comunicaciones de cualquier cliente, siempre y cuando el servicio de encriptado haya sido proporcionado por la compañía.

Esta norma no es aplicable por ejemplo a los servicios de mensajería móvil globales más populares, a pesar de que sus usuarios vivan en el territorio salvadoreño, al no ser un servicio manejado y ofrecido por las compañías que operan en el país. Esta ley ofrece una descripción clara de lo que es encriptado: sistema mediante el cual, con la ayuda de técnicas diversas o programas informáticos, se cifra o codifica determinada información con la finalidad devolverla inaccesible o ininteligible a quienes no se encuentran autorizados para tener acceso a ella.

Otra norma que menciona el encriptado en el ordenamiento jurídico salvadoreño es la Ley especial de Telecomunicaciones. En el apartado de material no descodificado, menciona el procedimiento que deben seguir los entes investigativos en caso de no poder decodificar un material encriptado. Ambas leyes presentan ciertos principios que buscan salvaguardar los derechos humanos, compromisos internacionales, y las garantías de los ciudadanos cómo lo son el derecho a la privacidad e intimidad, específicamente la privacidad, la temporalidad, la reserva y la confidencialidad.

105 Redacción. (2022). El Salvador: AI confirma uso de Pegasus para vigilar a periodistas. *DW*. https://www.dw.com/es/el-salvador-ai-confirma-uso-de-pegasus-para-vigilar-a-periodistas/a-60405648

106 Gordon Guerrel, I. (2019). ¿Qué es el sistema Pegasus?. La Estrella de Panamá. https://www.laestrella.com.pa/nacional/191107/sistema-pegasus

Cabe mencionar que El Salvador es uno de los países en Centroamérica donde la protección de datos personales no se ha desarrollado a través de un texto único, dejando de considerar nuevas reglas para la custodia y transferencia de los mismos. Durante la pandemia se discutió una iniciativa de ley con el objetivo que el titular de los mismos y partes interesadas puedan tener un balance entre el respeto de sus derechos en línea, sin frenar el desarrollo de Internet, el uso efectivo de las telecomunicaciones y el avance de las tecnologías de la información y comunicación, sin embargo, no fue sancionada por el nuevo gobierno con el compromiso de presentar y aprobar una ley de datos personales próximamente.

En el caso de Cuba, el encriptado y su regulación ha sido más polémico. En 2008 se aprobó una resolución que contemplaba una prohibición expresa de la criptografía por parte del Ministerio de la Informática y las Comunicaciones.[107] Sin embargo, una reforma del 2011 y 2017 permiten el uso de encriptado a través de un permiso que recibe el proveedor de internet.[108]

A razón de esta regulación excesiva violatoria de la privacidad de las comunicaciones, el Relator Especial para la Libertad de Opinión y Expresión de la Organización de Naciones Unidas criticó en el 2015 mediante un informe la resolución. En su informe el relator expresa que el regular el cifrado no permite el libre ejercicio de la opinión, además de dejar que el gobierno pueda intervenir las comunicaciones de sus ciudadanos[109].

A pesar de esta prohibición, el uso de plataformas de mensajería instantánea como WhatsApp y Telegram son ampliamente utilizadas en la isla. En 2020, Telegram estuvo bloqueado unas cinco semanas.[110] La situación se repitió en 2021, en medio de las mayores protestas desde 1959, el gobierno bloqueó muchas aplicaciones con cifrado en las redes 3G y 4G además de dejar sin internet a la isla.[111] En este mismo año, el gobierno presentó un Decreto ley que menciona multas a quienes utilicen encriptado sin la debida inscripción.[112] Esta nueva ley encendió nuevamente los debates internacionales y las condenas de gobiernos y organizaciones de sociedad civil por las violaciones a los derechos humanos.[113]

Activistas de derechos humanos han denunciado la mala práctica de empresas de revelar datos personales.[114] Durante 2022 se aprobó una ley de datos personales que entrará en vigencia en 2023, siendo criticada por su ambigüedad respecto a las excepciones de tratamiento sobre consentimiento del titular, específicamente “por razones de seguridad

---

107 Resolución NO. 179/2008. Reglamento para los Proveedores de Servicios de Acceso a Internet al Público. Ministerio de la Informática y las Comunicaciones. https://www.informatica-juridica.com/resolucion/resolucion-no-179-2008-proveedores-de-servicios-de-acceso-a-inter-net-al-publico/

108 Resolución no. 255/2017. Proveedor de Servicios de Acceso a Internet al PúblicoMinisterio de Comunicaciones.https://docplayer.es/113971827-Resolucion-no-255-2017.html

109 Cartaya, R. (2015). Crítica Relator de ONU control a cifrado de datos personales en Cuba. *Radio Martí.* https://www.radiotelevisionmarti.com/a/cuba-internet-derechos-encriptacion/97366.html

110 https://www.14ymedio.com/cuba/Telegram-funcionar-Cuba-intensa-denuncias_0_2968503124.html

111 Freedom on the Net: Cuba. (2022). Freedom House. https://freedomhouse.org/country/cuba/freedom-net/2022#footnote2_ Decreto Ley c07y586

112 No. 35 de 2021. De las telecomunicaciones, las tecnologías de la información y la comunicación y el uso del espectro radioeléctrico. Ministerio de Justicia. http://media.cubadebate.cu/wp-content/uploads/2021/08/goc-2021-o92-comprimido.pdf

113 Redacción. (2021). Cuba: Decreto de telecomunicaciones cercena la libertad de expresión. *Human Rights Watch.* https://www.hrw.org/es/news/2021/08/25/cuba-decreto-de-telecomunicaciones-cercena-la-libertad-de-expresion

114 ¿Sabías que en Cuba tenemos ejemplos de violación de privacidad? *Dominio Cuba*. https://www.youtube.com/watch?v=nhKo-jgRp5_A

colectiva, bienestar general, respeto al orden público e interés a la defensa".[115]

En el caso de Nicaragua y Panamá encontramos que en ninguno de los dos países se menciona en su regulación nacional el encriptado. Ambos países mantienen a nivel constitucional la privacidad de las comunicaciones y mantienen leyes de datos personales. En el caso de Nicaragua, su ley de datos personales no es aplicada y el órgano rector no está operativo.

Respecto a la norma legal, se puede interceptar comunicaciones de cualquier clase si cumple con ciertas características relativas al delito investigado si cuenta con una orden judicial.[116] A pesar de ello, se puede interceptar las comunicaciones aún sin la orden, después que durante las siguientes 24 horas sea recibida la solicitud por un juez[117]. En ese mismo sentido, una iniciativa de 2015 proponía obligar a las empresas proveedoras de internet a dar acceso a cualquier información que el gobierno nicaragüense deseara.[118] La iniciativa fue eliminada después de críticas de opositores y la sociedad civil.

Durante la pandemia, un informe de LACNIC determinó la urgencia de minimizar la injerencia de las autoridades en las comunicaciones e impulsar el uso del cifrado y redes seguras de comunicación en el país.[119] Durante las protestas de 2018, se reportaron situaciones en los que la Policía obligaba a protestantes a desbloquear sus celulares para leer sus conversaciones sin importar el encriptado.[120]

Periodistas y defensores de derechos humanos reportan la importancia del encriptado para sus labores y activismo a pesar de las limitantes que presentan las plataformas al ejercicio periodístico.[121] En el caso de Panamá existe una ley de protección de datos personales de reciente promulgación y entrada en vigencia. De igual forma, su norma penal permite la interceptación de comunicaciones con una resolución judicial motivada.[122] A diferencia de los demás países analizados, el acoso periodístico común es de tipo judicial hasta el momento.[123]

---

115 Emil, E. (2022). Cuba: datos personales y una ley a conveniencia del poder. *CUBALEX*. https://cubalex.org/2022/10/11/cuba-datos-personales-y-una-ley-a-conveniencia-del-poder/

116 Código procesal penal, Ley No. 406. http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/5EB5F629016016CE062571A1004F7C62?OpenDocument

117 Morales Angulo, C. (2021)¿Quién defiende tus datos? Nicaragua 2020. *IPANDETEC*. https://www.ipandetec.org/wp-content/uploads/2020/12/QDTD-nicaragua-2020-1.pdf

118 Salinas Maldonado, C. (2015). El Gobierno de Nicaragua crea una ley para controlar Internet. *El País*. https://elpais.com/internacional/2015/05/13/actualidad/1431535413_014757.html

119 Gonzalez, O. (2021) Cifrado de datos en Nicaragua. *LACNIC*. https://descargas.lacnic.net/lideres/oscar-gonzalez/oscar-gonzales.pdf

120 Fonseca, R. (2018). Nicaragua: Fuerzas policiales revisan ahora celulares de periodistas y ciudadanos. *Onda Local*. https://ondalocal-ni.com/noticias/442-nicaragua-fuerzas-policiales-revisan-ahora-celulares-de-periodistas-y-ciudadanos/

121 Redacción. (2021). El desafío de usar WhatsApp, una plataforma no diseñada para medios. *Confidencial*. https://www.confidencial.digital/nacion/el-desafio-de-usar-whatsapp-una-plataforma-no-disenada-para-medios/; Presuma que toda comunicación está intervenida: ¿Cómo enfrentar el espionaje del régimen Ortega-Murillo? (20222). *Despacho 505*. https://www.despacho505.com/presuma-que-toda-comu-nicacion-esta-intervenida-como-enfrentar-el-espionaje-del-regimen-ortega-murillo/ ; Redacción Confidencial. (2022). La guerra de Daniel Or-tega contra el periodismo: 54 medios cerrados. *Confidencial*. https://www.confidencial.digital/politica/54-medios-cerrados-guerra-daniel-or-tega-periodistas-en-nicaragua/

122 Código Penal de Panamá. https://www.gacetaoficial.gob.pa/pdfTemp/27446_B/44985.pdf

123 Redacción EFE. (2022). SIP advierte que se mantiene un acoso judicial a la prensa en Panamá. SwissInfo. https://www.swissinfo.ch/spa/sip-asamblea-panam%C3%A1_sip-advierte-que-se-mantiene-un-acoso-judicial-a-la-prensa-en-panam%C3%A1/48017238

Además, el encriptado fue utilizado durante la pandemia por las autoridades para diseñar productos en respuesta a la pandemia del covid-19.[124] Por otro lado, en 2021 se reportó una filtración de un proyecto de fallo encriptado perteneciente a uno de los magistrados de la Corte Suprema de Justicia.[125] El proyecto correspondía a una acción de inconstitucionalidad relativa a un expresidente del país acusado de violar las comunicaciones. Las anteriores son dos de las pocas situaciones a nivel nacional donde se menciona el cifrado.

Por otro lado, el cifrado es mencionado como garante de la sexualidad de minorías sexuales por Internet Society.[126] El personal médico utiliza cifrado para comunicarse con pacientes trans con el fin de que se sientan seguros de que su información no será filtrada. De igual forma, protege a personas LGBTQIA+ de sufrir discriminación al elegir si desean compartir su orientación o identidad de género y ayuda que adolescentes y jóvenes que viven en países donde sus orientaciones sexuales son prohibidas puedan comunicarse con pares en otros países. En el caso de los países estudiados, ser una persona LGBTQIA+ no es prohibido, sin embargo, existe una amplía discriminación. Cuba es el único que permite el matrimonio igualitario, por lo que es conclusivo opinar que las personas LGBTQIA+ de Cuba, Nicaragua, Panamá y El Salvador utilizan servicios de mensajería cifrado por su seguridad. Esto deja demostrado que además de los derechos anteriormente mencionados asegura los derechos de autodeterminación e identidad.

• Conclusión

Después del anterior análisis no queda duda que el encriptado asegura derechos humanos vitales y la necesidad de que los gobiernos y las sociedades hagan todo lo posible por asegurar su funcionamiento.

En los casos estudiados podemos ver cómo el cifrado va cambiando según el régimen político del país. Los derechos de privacidad, libertad de expresión, asociación y datos personales se encuentran consagrados de forma directa o indirecta en todas las Constituciones del continente, por lo que los derechos humanos se mezclan con lo político en el caso del uso de las nuevas tecnologías.

Desde dictaduras cómo la cubana donde se controla el cifrado, pasando a un régimen autoritario sin recursos para darle seguimiento al cifrado como Nicaragua, examinamos también la democracia cambiante de El Salvador, para finalmente analizar una democracia de libertades plenas como Panamá donde no se regula el cifrado.

Al mismo tiempo se puede entender que en los países donde no existe ninguna mención del cifrado o encriptado en la regulación existe su uso extendido. Es el caso de Panamá donde hay un apoyo tácito de su uso a nivel gubernamental.

Por otro lado, la libertad de prensa se ve salvaguardada gracias al encriptado. Periodistas acuden a esta tecnología para proteger sus fuentes e investigaciones de personas

124 Calderon Sanchez, A. (2021). AIG: información del Código QR está encriptada. *EcoTV*. https://www.ecotvpanama.com/radiografia/programas/aig-informacion-del-codigo-qr-esta-encriptada-n5341186

125 Redacción. (2021). Filtración de fallo debe castigarse. Panamá América. https://www.panamaamerica.com.pa/judicial/filtra-cion-de-fallo-debe-castigarse-1195928

126 Redacción. (2019). Cifrado: imprescindible para la comunidad LGTBI. Internet Society y LGBT Tech. https://www.internetsociety.org/es/resources/doc/2019/encryption-factsheet-essential-for-lgbtq-community/

opositoras o actores gubernamentales, sobre todo en gobiernos autoritarios como el de Nicaragua.

Al mismo tiempo, pudimos ver otros derechos salvaguardados cómo el derecho a la autodeterminación e identidad de las personas LGBTQIA+.

• Recomendaciones

Es necesario que los gobiernos analizados respeten la privacidad de las comunicaciones a través del respeto de las leyes garantes vigentes y la formulación de políticas públicas que busquen ese garantismo.

Por otro lado, algunos de los países analizados, cómo Cuba y El Salvador deben reformar sus leyes actuales o derogarlas dando pasó a nuevos textos legales con estándares de derechos humanos.

De igual forma, es necesaria la discusión o actualización de leyes que protejan los datos personales en la región.

Por último, los gobiernos deben hacer todo lo posible para difundir el encriptado para minorías étnicas y raciales, defensores de derechos humanos y periodistas. Hacerlo supone un compromiso con la democracia.

País: Venezuela

Autor: Rómulo Chacín González

El cifrado en Venezuela: Impacto de las políticas en los derechos fundamentales

• Introducción

A nivel mundial existe una tendencia cada vez más frecuente de parte de los gobiernos y de los ciberdelincuentes a tener acceso a información de terceros por múltiples razones. Sin embargo, el caso de Venezuela es especialmente alarmante en la región habida cuenta de que la violación de los derechos fundamentales es una práctica institucionalizada y sistemática, dando lugar a la comisión de crímenes de lesa humanidad.

La configuración del escenario es propicio para ello pues, además, no existen instituciones imparciales y efectivas que protejan al individuo frente a estos atropellos, así como tampoco existe una legislación robusta en materia de protección de datos personales. En contraste con esto, sí existe una gran cantidad de agencias de inteligencia creadas por Decretos del Poder Ejecutivo que operan a discreción del régimen, cuyas facultades son ambiguas y permiten ser acomodadas en perjuicio de los individuos, en abierta contradicción con los principios de legalidad, necesidad, proporcionalidad y debido proceso.

Ante tal escenario, el uso del cifrado se erige como un derecho que cuenta con cobertura constitucional y como una necesidad de las personas para evadirse de la incesante vigilancia estatal, así como de la ciberdelincuencia; pues éste tiende a garantizar la privacidad de las comunicaciones y de la información en general.

Por todo ello, con el presente informe se propone realizar un estudio de las acciones más relevantes desplegadas en Venezuela, tanto a favor del cifrado como en contra de éste, a los fines de determinar su impacto en los derechos de los individuos, fundamentalmente en la libertad de expresión, privacidad, protección de datos personales, y seguridad.

• Metodología

La investigación realizada fue de tipo documental con revisión crítica del estado del conocimiento, a nivel exploratorio. El proceso se basó en la búsqueda, recolección, análisis, crítica e interpretación de datos e información contenida en fuentes documentales impresas y electrónicas, fundamentalmente en informes de instituciones privadas venezolanas y de organizaciones de Derechos Humanos, así como de normas jurídicas relacionadas de forma directa o indirecta con el cifrado. Con ello se pretende el desarrollo de este tema en Venezuela atendiendo a su escaso estudio.

• Contexto y antecedentes

Venezuela atraviesa desde el año 2014 una de las más profundas y complejas crisis a nivel global, especialmente en lo que respecta a la situación de los Derechos Humanos. Torturas, desapariciones forzadas, ejecuciones extrajudiciales, detenciones arbitrarias,[127] requisas ilegales e interceptación de comunicaciones, son algunas herramientas de uso cotidiano por parte de las autoridades y sus colaboradores. El derecho a la privacidad ha sido uno de los más afectados a través de la vigilancia que ejercen sobre las comunicaciones las agencias de inteligencia del Estado, CONATEL y CANTV por razones políticas.[128] De hecho, es común escuchar conversaciones privadas grabadas en los canales de televisión del gobierno para dejar en evidencia a los afectados, lo cual es una muestra de la gravedad de esta situación.

En relación con lo anterior, el sector privado[129] también ha sido partícipe de estas conductas de vigilancia a pedido de las agencias del régimen. En 2021, Telefónica interceptó 1.584.547 líneas en Venezuela,[130] cifra que evidencia un claro y constante aumento desde 2016. Como bien apunta Vesinfiltro,[131] esto equivale a más del 20% de sus suscriptores en el país, siendo que en el resto de naciones en las cuales tiene operaciones la compañía, esta cifra no logra alcanzar ni el 1%.

Otra poderosa herramienta del Estado para la intervención en la esfera de libertades del individuo es la censura. Al respecto, Espacio Público estima que entre los años 2003 y 2022 se han cerrado al menos 215 emisoras de radio a nivel nacional. De hecho, la censura alcanzó el 39% de las violaciones a la libertad de expresión en 2022.[132]

Estos hechos se unen a otros igualmente graves como el bloqueo de Tor y de otras herramientas para la evasión de la censura como redes privadas virtuales, así como del protocolo de comunicación *Hypertext Transfer Protocol Secure* (HTTPS)[133] en algunos sitios web[134] que fungen como medios de comunicación e información. Vale destacar que todas estas tecnologías hacen un importante uso del cifrado.

---

127 Human Rights Watch. (2022). *World Report 2022*. Disponible en https://www.hrw.org/es/world-report/2022/country-chapters/380706

128 Privacy International. (2016). *The Right to Privacy in Venezuela*. Disponible para su consulta en https://www.privacyinternational.org/sites/default/files/2017-12/venezuela_upr2016.pdf.

129 Departamento de Estado. (2020). *Country Reports on Human Rights Practices: Venezuela.* Disponible para su consulta en https://www.state.gov/wp-content/uploads/2021/10/VENEZUELA-2020-HUMAN-RIGHTS-REPORT.pdf. p.17.

130 Telefónica. (2022). *Informe de Transparencia en las Comunicaciones 2021*. Disponible para su consulta en https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/08/Informe-de-Transparencia-en-las-Comunicaciones-2021.pdf

131 Vesinfiltro. (2022). *Espionaje masivo de las comunicaciones en Venezuela*. Disponible para su consulta en https://caleidohumano.org/el-gobierno-de-venezuela-espia-de-forma-masiva-las-comunicaciones-privadas-en-el-pais/.

132 Espacio Público. (2022). *Situación General del Derecho a la Libertad de Expresión Enero-Agosto 2022*. Disponible para su consulta en https://espaciopublico.ong/situacion-general-del-derecho-a-la-libertad-de-expresion-enero-agosto-2022/amp/.

133 Departamento de Estado. (2021). *Country Reports on Human Rights Practices: Venezuela.* Disponible para su consulta en https://www.state.gov/wp-content/uploads/2022/02/313615_VENEZUELA-2021-HUMAN-RIGHTS-REPORT.pdf. p. 28.

134 Recientemente, la Alta Comisionada para los Derechos Humanos de Naciones Unidas hizo énfasis en el bloqueo de al menos siete sitios web pertenecientes a medios de comunicación en Venezuela. Ver en https://www.ohchr.org/en/statements-and-speeches/2022/03/high-commissioner-updates-human-rights-council-venezuela.

No en vano, Venezuela fue catalogada como uno de los países con menor libertad de internet en el mundo con una valoración de 30/100 puntos,[135] calificación que la hace acreedora del penúltimo lugar en toda Latinoamérica en este particular.

• Políticas Relacionadas con el Cifrado

La inviolabilidad de las comunicaciones privadas se encuentra consagrada en la Constitución de la República Bolivariana de Venezuela[136] (CRBV) en su Art. 48, el cual, garantiza el secreto e inviolabilidad de estas en todas sus formas. Así las cosas, tanto personas naturales como jurídicas gozan del derecho a la confidencialidad de su contenido, de forma tal que la información sea inaccesible por terceros no deseados, implicando en consecuencia que solo aquellos autorizados puedan acceder a ella.

En relación con ello, conviene destacar que todas las personas son titulares de este derecho sin importar el medio de comunicación, el cual, puede ser escrito, informático, sonoro, entre otros; y que dichas comunicaciones solo podrán ser intervenidas mediando la orden judicial correspondiente.

Por otra parte, el Art. 60 *ejusdem* reconoce los derechos a la protección del "*honor, vida privada, intimidad, propia imagen, confidencialidad y reputación*." Del contenido de estas dos normas de rango constitucional se deriva la facultad de los individuos presentes en el territorio de la República de proteger sus comunicaciones y, en general, cualquier tipo de información a través de los medios que estimen apropiados para tal fin. Como resulta obvio concluir, el cifrado es uno de ellos.

En el numeral 2 del Art. 12 de la Ley Orgánica de Telecomunicaciones[137] se reconoce el derecho de los usuarios a la privacidad e inviolabilidad de las telecomunicaciones, exceptuando aquellos casos expresamente autorizados por la CRBV o que tengan carácter público.

Su Reglamento para la Protección de los Derechos de los Usuarios en la Prestación de los Servicios de Telecomunicaciones (2018)[138] establece en su Art. 7 el deber de los operadores de establecer mecanismos para resguardar el secreto e inviolabilidad de las comunicaciones privadas que cursen en sus redes. Del mismo modo, su Art. 30 señala que estos deberán adoptar mecanismos que garanticen la confidencialidad de los datos personales.

El numeral 2 del Art. 18 de la Ley Orgánica de Reforma Parcial del Decreto con Rango, Valor y Fuerza de Ley Orgánica de Ciencia, Tecnología e Innovación[139] establece que la autoridad nacional con competencia en estas materias, deberá resguardar la inviolabilidad del carácter confidencial de los datos electrónicos obtenidos en el ejercicio de las funciones

---

135 Freedom House. (2022). ***Freedom on the Net***. Disponible para su consulta en https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf.

136 Publicada en la Gaceta Oficial Nro. 5.908 Extraordinario del 19 de febrero de 2009. Disponible para su consulta en http://www.sudeban.gob.ve/wp-content/uploads/Recursos/Constitucion.pdf.

137 Publicada en la Gaceta Oficial Nro. 39.610 del 7 de febrero de 2011. Disponible para su consulta en https://www.asambleanacional.gob.ve/storage/documentos/leyes/ley-de-ref-20220117162719.pdf.

138 Disponible para su consulta en http://www.conatel.gob.ve/reglamento-para-la-proteccion-de-los-derechos-de-los-usuarios-en-la-prestacion-de-los-servicios-de-telecomunicaciones/

139 Publicada en la Gaceta Oficial Nro. 6.693 Extraordinario del 1 de abril de 2022. Disponible para su consulta en https://www.asambleanacional.gob.ve/storage/documentos/leyes/ley-de-ref-20220609123842.pdf.

de los órganos y entes públicos. También, en el numeral 22 del Art. 19 dispone entre las competencias del órgano rector la de establecer las políticas, normas y medidas técnicas orientadas a resguardar la privacidad, confidencialidad e inviolabilidad de las personas.

En relación con ello, el Centro Nacional de Tecnologías de Información publicó en el año 2011 el Marco de Interoperabilidad (MIO) para integrar los servicios del Estado, otorgando una gran importancia al cifrado como componente de la capa de seguridad en el intercambio electrónico de datos entre sus instituciones[140].

La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) también hace un fuerte uso del cifrado como método para resguardar las copias de seguridad de las claves privadas y para la exportación de la misma a otros componentes del sistema[141].

Por su parte, los Arts. 23 y 25 de la Ley de Infogobierno[142] establecen tanto el principio de seguridad como la protección de los datos personales, en relación con el uso de las tecnologías de información por parte del Poder Público y el Poder Popular. Al respecto, se debe garantizar la integridad, confidencialidad, autenticidad, y disponibilidad de la información, documentos y comunicaciones electrónicas. Además, el segundo de ellos establece el deber de respeto del honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas. Por otra parte, en su Art. 55.4 se asigna a SUSCERTE la articulación e inserción de iniciativas en materia de seguridad informática.

El Art. 173 del Decreto con Rango, Valor y Fuerza de Ley de Instituciones del Sector Bancario[143] establece las atribuciones y funciones en materia de seguridad bancaria que ostenta la Superintendencia de las Instituciones del Sector Bancario. Entre ellas, destaca en su numeral 1 la de velar porque dichas instituciones dispongan de los sistemas y procedimientos necesarios para minimizar la presencia de fraudes en sus operaciones.

De acuerdo a éste, en el Art. 20 de la Resolución Nro. 641-10[144] de la citada Superintendencia, de fecha 23 de diciembre de 2010, se estableció que estos deben emplear un cifrado robusto para proteger el canal de comunicación. En igual sentido, se dispuso en su Art. 21 que dichas instituciones deben implementar mecanismos de cifrado en la transmisión y almacenamiento de la información, a fin de evitar que los datos sensibles sean conocidos por terceros no autorizados para ello. Esto fue reafirmado en el literal "m" del Art. 23 en su Resolución Nro. 001.21, de fecha 4 de enero de 2021.

Otros textos normativos que abordan el tema de la confidencialidad, integridad privacidad y, en general, la seguridad de las comunicaciones y de los datos e información, son el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas,[145] el Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos,

---

140 Disponible para su consulta en https://www.cnti.gob.ve/phocadownload/publicaciones/mio.pdf.

141 Disponible para su consulta en http://www.suscerte.gob.ve/dpc/DPC.pdf.

142 Publicada en la Gaceta Oficial Nro. 40.274 del 17 de octubre de 2013. Disponible para su consulta en https://www.asambleanacional.gob.ve/leyes/sancionadas/ley-de-infogobierno.

143 Publicado en la Gaceta Oficial Nro. 40.557 del 8 de diciembre de 2014. Disponible para su consulta en https://www.asambleanacional.gob.ve/storage/documentos/leyes/decreto-n0-1402-mediante-el-cual-se-dicta-el-decreto-con-rango-valor-y-fuerza-de-ley-de-instituciones-del-sector-bancario-20211026183241.pdf.

144 Este texto normativo define al cifrado o encriptación como el "*proceso de convertir en ilegible un mensaje que se encuentra en texto claro, usualmente mediante la utilización de algoritmos matemáticos y una clave.*"

145 Publicado en la Gaceta Oficial Nro. 37.148 del 28 de febrero de 2001. Disponible para su consulta en https://www.asambleanacional.gob.ve/storage/documentos/leyes/decreto-no-20220315144506.pdf.

Información y Documentos entre los Órganos y Entes del Estado,[146] así como la Ley sobre Protección a la Privacidad de las Comunicaciones.[147]

En otro orden de ideas, vale destacar que si bien Venezuela no cuenta con una legislación integral en materia de protección de datos personales, la Sala Constitucional de nuestro máximo tribunal[148] dispuso importantes pautas que deben ser observadas en relación con "*…toda normativa o sistema sobre datos personales que contenga información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables…*". Entre sus aspectos más relevantes, resalta el principio de seguridad y confidencialidad, de acuerdo al cual, "*deberán adoptarse las medidas técnicas y organizativas que resulten necesarias para proteger los datos contra su adulteración, pérdida o destrucción accidental, el acceso no autorizado o su uso fraudulento.*"

La aplicación móvil WhatsApp es, quizás, la herramienta de comunicación más usada en Venezuela en lo que a mensajería personal y llamadas se refiere. Su uso es tan importante en el país, que es considerado un canal de información para la mayoría de la población[149] en virtud de la desinformación imperante. Dicha aplicación, emplea un mecanismo de cifrado asimétrico de extremo a extremo desde el año 2016, lo cual, implica que nadie pueda tener acceso al contenido de las comunicaciones (video, audio, imágenes, archivos, llamadas, videollamadas o mensajes) en formato legible, garantizando así su confidencialidad como atributo de la seguridad de la información.[150] Otras aplicaciones similares ampliamente utilizadas son Telegram y Signal.

Los particulares también se benefician del cifrado al realizar pagos en la nube[151] y transacciones bancarias,[152]así como al navegar por internet gracias al protocolo HTTPS. El mismo, es promovido por organizaciones como WordPress Venezuela[153] y en general, el cifrado es auspiciado por ONG's como ISOC Venezuela y Vesinfiltro.

En abierta contradicción con todo lo anterior, destaca la gran cantidad de agencias de inteligencia del Estado y la indeterminación de sus facultades en Decretos que restringen las libertades; el marco normativo digital ambiguo y disperso, la precariedad de las regulaciones relativas a la protección de datos personales y la ausencia absoluta de mecanismos de control efectivos e imparciales. Esto configura, sin lugar a dudas, un entorno propicio de vigilancia en el que se hace fácil enfriar la libertad de expresión, dañando gravemente el entorno necesario para una sociedad democrática.[154]

---

146 Publicado en la Gaceta Oficial Nro. 39.945 del 15 de junio de 2012. Disponible para su consulta en https://www.asambleanacional.gob.ve/storage/documentos/leyes/decreto-n0-9051-mediante-el-cual-se-dicta-el-decreto-con-rango-valor-y-fuerza-de-ley-sobre-acceso-e-intercambio-electronico-de-datos-informacion-y-documentos-entre-los-organos-y-entes-del-estado-20211108195715.pdf.

147 Publicada en la Gaceta Oficial Nro. 34.863 del 16 de diciembre de 1991. Disponible para su consulta en https://www.asambleanacional.gob.ve/storage/documentos/leyes/ley-sobre--20220401155924.pdf.

148 Ver en su sentencia vinculante Nro. 318 del 4 de agosto de 2.011.

149 Espacio Público. (2022). *Privacidad y Datos Personales en Venezuela*. Disponible para su consulta en https://espaciopublico.ong/wp-content/uploads/2022/01/Informe-Privacidad-y-datos-personales-en-Venezuela-Enero-2022.pdf . p.17.

150 Ver *WhatsApp Encryption Overview: Technical white paper*, disponible para su consulta en https://faq.whatsapp.com/791574747982248/?locale=es_LA.

151 Ver en https://www.cavedatos.org.ve/noticias/el-cifrado-para-pagos-en-la-nube-llega-a-venezuela/ .

152 Ver en https://www.banesco.com/personas/banca-digital-personas/banca-en-linea/banesconline-naturales. En el mismo, Banesco indica que "Al ingresar al servicio de BanescOnline, tus datos se transmiten a nuestros servidores utilizando la tecnología TLS en su versión 1.2, la cual garantiza la privacidad de tu información para que no pueda ser leída por personas sin autorización."

153 Ver en https://ve.wordpress.org/support/article/why-should-i-use-https/

154 Derechos Digitales. (2018). *Políticas Públicas para el Acceso a Internet en Venezuela*. Disponible para su consulta en https://www.derechosdigitales.org/wp-content/uploads/CPI_venezuela.pdf

Existe evidencia razonable para creer que la firma israelí Cellebrite vendió tecnología de piratería telefónica al régimen de Maduro aduciendo supuestos motivos de combate a la delincuencia. Vale destacar, que la herramienta en cuestión puede desbloquear y extraer datos de teléfonos móviles incluyendo los datos cifrados,[155] lo cual, genera gran preocupación debido al nivel exagerado de desprecio de los Derechos Humanos en Venezuela.

Si bien no se evidencia una conducta generalizada y sistemática en contra del cifrado, es necesario poner de relieve que varias redes privadas virtuales (VPN) han sido bloqueadas por CANTV y algunos proveedores privados,[156] toda vez que estas han sido utilizadas por la población como forma de evitar la censura a diversos medios y la vigilancia estatal. Ejemplos de algunas de estas redes bloqueadas son TunnelBear y Psiphon.[157]

Además, también hay evidencia de que Venezuela inició negociaciones tendientes a la adquisición de *Remote Control System* (RCS) de *Hacking Team* en el año 2013, herramienta que permite tener acceso a correos y comunicaciones cifradas.[158]

Entre los más afectados por estas prácticas abusivas del Estado venezolano, se encuentran activistas,[159] defensores de derechos humanos, políticos y cualquier persona que tenga alguna vinculación política contraria al régimen. Sin embargo, como bien puede apreciarse en el informe de Telefónica antes comentado, todas las personas son realmente un objetivo potencial de estas acciones.

• Conclusión

La protección de las comunicaciones y, en general cualquier tipo de información, es un derecho que cuenta con cobertura constitucional en Venezuela, así como con un desarrollo normativo de rango legal y sub legal. Dicha protección puede ser realizada a través de cualquier medio, incluyendo el cifrado. Si bien son pocas las normas que lo aluden de forma expresa, ello no obsta para considerar que su uso, al igual que el de otras herramientas y técnicas de seguridad, es un derecho que surge de la inviolabilidad de las comunicaciones privadas y del derecho a la protección personal.

Es inexistente un marco jurídico sólido en lo que respecta a la protección de datos personales, lo cual nos aleja de los estándares internacionales en la materia y deja a las personas en situación de vulnerabilidad ante la ausencia de mecanismos e instituciones especializadas, imparciales y efectivas.

---

155 Freedom House. (2022). *Libertad en la Red: Venezuela*. Disponible para su consulta en https://freedomhouse.org/country/venezuela/freedom-net/2022.

156 Vesinfiltro. (2021). ***Report: Digital rights, censorship, and connectivity in Venezuela***. Disponible para su consulta en https://vesinfiltro.com/noticias/2021_annual_report/.

157 Aragort, D. (2022). *Enfoques no centrados en el Usuario para Enfrentar la Censura en Internet en Venezuela*. Disponible para su consulta en https://www.youtube.com/watch?v=r01C-Or7PjM

158 Derechos Digitales. (2016). *Informe: Hacking Team Malware para la Vigilancia en América Latina*. Disponible para su consulta en https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf . p.9.

159 AC-LAC. (2022). *Cifrado y Derechos Humanos: Cómo Protege el Cifrado los Derechos de las Minorías*. Disponible para su consulta en https://ac-lac.org/wp-content/uploads/2022/06/Gu%C3%ADa-CIFRADO-Y-DERECHOS-HUMANOS-¿CÓMO-PROTEGE-EL-CIFRADO-LOS-DERECHOS-DE-LAS-MINORÍAS.pdf .p.5.

Los ataques a las libertades son de uso común en nuestra región; sin embargo, el caso de Venezuela es especialmente alarmante y la situación es favorable para las prácticas abusivas del Estado. La innumerable cantidad de agencias de inteligencia del régimen, un Poder Judicial ineficiente al servicio de éste y la politización generalizada del acceso a los bienes y servicios; son algunos de los elementos esenciales para ello.
No se evidencia una conducta generalizada y sistemática que apunte especialmente contra el cifrado en Venezuela; no obstante, ello sí es predicable de la censura y de la vigilancia como políticas institucionalizadas. Algunas de estas políticas han logrado impactar de forma negativa en el cifrado.

Todo lo anterior, aunado a la desconfianza generalizada de la población con respecto a las instituciones públicas y sus representantes, hacen del cifrado una poderosa y necesaria herramienta de protección de la información y de las comunicaciones, para hacer frente no sólo a las prácticas abusivas del Estado, sino además a las actividades maliciosas de los ciberdelincuentes.

• Recomendaciones

Se insta a todos los órganos y entes del Poder Público en todos sus niveles a que protejan y promuevan el uso del cifrado fuerte de extremo a extremo a través de las políticas correspondientes, pues ello tiende a garantizar la seguridad de millones de personas, así como la seguridad del país. Así las cosas, debe abandonarse cualquier práctica que vulnere directa o indirectamente al cifrado.

Se recomienda a todas las personas la adopción del cifrado fuerte en lo que respecta a su información y comunicaciones, pues es la herramienta más sólida disponible para la protección de estos últimos. En especial, ello se recomienda para activistas, defensores de los Derechos Humanos, periodistas y para todo aquel vinculado de forma directa o indirecta con actividades políticas.

Se urge al Poder Legislativo a discutir y aprobar una ley de protección de datos personales que desarrolle las normas constitucionales en la materia y que sea conforme con los estándares internacionales de protección. También, es importante realizar una revisión exhaustiva de las normas y prácticas que restringen la libertad de expresión y el derecho a comunicarse libremente y, en todo caso, modificarlas para que acaten los principios de legalidad, necesidad, proporcionalidad y debido proceso.