Relatório regional sobre políticas e liberdades no uso de criptografia na América Latina e no Caribe

Realização

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

Coordenação e Revisão

Mariana Canto
Raquel Saraiva
Michel Souza

Tradução

Fernanda Lobo

Idealização

André Ramiro

Projeto gráfico

Clara Guimarães

O IP.rec utilizou recursos do WhatsApp LLC. para produzir este informe.

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

Relatório regional sobre políticas e liberdades no uso de criptografia na América Latina e no Caribe [livro eletrônico] / coordenação Mariana Canto, Raquel Saraiva, Michel Souza. -- Recife, PE : IP.rec, 2023.
PDF

Vários autores.
ISBN 978-65-995947-7-9

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.

23-151924 CDU-342.721

Índices para catálogo sistemático:

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

Sumário

INTRODUÇÃO

O debate sobre criptografia ao redor do mundo continua sendo enquadrado como uma tensão entre, de um lado, segurança da informação e privacidade das comunicações e, de outro, acessibilidade para investigações criminais e aplicação da lei e para fins de segurança nacional. Buscando entender como conjunturas políticas relacionadas ao uso e desenvolvimento da criptografia têm impactado direitos na região, o "Relatório regional sobre políticas e liberdades no uso de criptografia na América Latina e no Caribe" expõe o estado das políticas públicas e do nível de liberdade sobre o uso de tecnologias com criptografia na região.

Fruto da parceria entre o Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec, através do Observatório da Criptografia - ObCrypto, e a Derechos Digitales, a publicação tem como fim expor, de maneira não-exaustiva, os diferentes riscos no legislativo, executivo e judiciário latinoamericano e caribenho para o uso e desenvolvimento de tecnologias com criptografia. Da mesma forma, oferece um mapeamento do estado das liberdades sobre o uso da criptografia na região e um termômetro sobre o exercício de direitos conexos ao pleno uso da criptografia, como a liberdade de expressão, opinião, manifestação e associação, privacidade, segurança e proteção de dados pessoais.

Assim, o projeto buscou a articulação com distintos relatores em países estratégicos da região, incluindo ativistas, organizações dedicadas à defesa dos direitos humanos no contexto de novas tecnologias, bem como membros da academia e pesquisadores. Agradecemos às contribuições feitas pelos nossos relatores, sem as quais esse relatório não seria possível, e que atuaram como especialistas necessários à construção de um panorama contemporâneo sobre o cenário legislativo e judiciário referentes ao tema, assim como fatos políticos e contextos de interesse na região.

Finalmente, a partir desta publicação, objetiva-se oferecer insumos necessários para ações de incidência sobre situações que alertem para restrições ao uso civil da criptografia, assim como fomentar novas pesquisas sobre o tema com um olhar latinoamericano e caribenho. Como resultado, o projeto visou criar um precedente documental de utilidade pública que reflita o status sobre a garantia de direitos humanos conexos ao uso da criptografia na América Latina.

País: Argentina

Autor: Lucas Domínguez Rubio

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

Notas para uma história recente da difusão da criptografia na Argentina (2010-2020)

• Introdução

Este relatório propõe percorrer os diferentes espaços que promoveram o uso de GnuPG, OTR y TOR na Argentina ou as discussões ao redor destas ferramentas para a criptografia de e-mails, mensageria e navegação. Refere-se, portanto, ao uso de criptografia que não tem que ser implementada diretamente pelas plataformas provedoras de serviços digitais para garantir a segurança de dados, serviços ou transações, mas a ferramentas usadas pelos de baixo por vontade ou necessidade dos próprios usuários.

Provavelmente foi em torno do ano 2010 quando se começaram a registrar as primeiras oficinas e textos que buscavam a difusão sistemática dessas ferramentas e suas discussões. Dez anos depois, a criptografia das comunicações nos serviços de mensageria mediante OTR ficou obsoleta. Mesmo que, no caso, as implementações privadas de criptografia de ponta-a-ponta impossibilite a auditoria, o uso massivo dos principais serviços de mensageria instantânea – como Whatsapp (Meta, ex-Facebook) e, em menor medida, Telegram e Signal – fez que o uso de OTR tenha desaparecido totalmente da discussão.[1]

No caso do TOR, as discussões se mantiveram sempre em níveis mínimos e, ainda que sua utilização envolva discussões e práticas totalmente diferentes, a extensão de serviços de VPN se converteu em uma alternativa parcial a ser utilizada com certos objetivos.[2] O número de nós TOR na Argentina oscilou entre 0 e 8 nos últimos dez anos. Nos seus extremos, em 2013 havia oito nós de saída, em 2017 havia 0, e em novembro de 2022 contamos com 8 nós, dos quais apenas 2 eram de saída.[3] Nem seu uso, nem suas discussões tiveram maiores repercussões, e apenas alguns casos pontuais chamaram a atenção pública.[4]

Por outro lado, se o e-mail constitui o meio mais utilizado para as comunicações formais, as principais organizações ativistas que impulsionam o tema não publicam suas chaves públicas em suas páginas de contato. Hoje em dia, o baixo uso de GnuPG combina-

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/ Nesse sentido, o uso do TOR na Argentina seguiu a tendência comum que se deu em nível global registrando um pico de uso no fim de 2013: https://metrics.torproject.org/userstats-relay-country.html?star-t=2010-08-23&end=2022-11-21&country=ar&events=off

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

se com novos modos de implementação em serviços de e-mail baseados na privacidade (sobretudo Protonmail e Tutanota). Os eventos específicos para trocar e consolidar mutuamente as respectivas chaves públicas de GnuPG – chamadas *criptoparties* – foram difundidas na Europa entre 2012 e 2019.[5] Mesmo que, nesse mesmo período na Argentina, tenham existido também algumas criptoparties, nas quais ainda se debatia e difundia o uso de TOR e OTR, em um ciclo semelhante, hoje em dia, elas também encontram-se descontinuadas.[6]

• Metodologia

Com o fim de alcançar um "relatório regional sobre políticas e liberdades no uso de criptografia na América Latina", faz-se fundamental conhecer as publicações e os modos de difusão que a promoção do uso da criptografia na Argentina. Nesse sentido, adota-se um foco embasado na história editorial e seus meios de difusão: oficinas, livros, revistas e plataformas web que difundiram os problemas relacionados à criptografia nos últimos anos permitem reconhecer discussões comuns. Quais foram os espaços a partir dos quais se promoveu o uso de criptografia em nível pessoal? Que textos e autores se usaram para embasar esse debate? É possível identificar estratégias locais específicas em nível nacional? Foram debates que se deram de maneira isolada ou vinculados a outros temas?

• Contexto e antecedentes

As publicações das diferentes plataformas colocadas em relevo mostram um arco de temas em comum que circularam como interesses compartilhados, sobretudo ao redor de dois eixos: privacidade/ criptografia e software livre/licenças *copyleft*. Trata-se de discussões, em larga medida, internacionais produzidas na década em que o uso da internet para todas as esferas da vida deu um salto quantitativo de enorme magnitude até se tornar imprescindível.

Dessa forma, as plataformas locais de visaibilização e discussão desses problemas se inscreviam em uma agenda global de referências, nomes e problemas de maior escala. Frente ao crescimento do uso de serviços digitais *mainstream* e o avanço pretensamente neutro da tecnologia em nível cotidiano, só alguns poucos espaços buscaram politizar o uso de software para se perguntar sobre as alternativas que se abriam.

• Difusão da criptografia na Argentina

A Fundação Vía Livre foi criada na cidade de Córdoba no ano de 2000, mas suas atividades ganharam visibilidade sobretudo a partir do ano de 2008 e se centralizaram na acidade de Buenos Aires. Seus interesses residiam na difusão do software livre e as licenças que potencializem a circulação do conhecimento[7] com campanhas contra o avanço da vigilância e a perda de privacidade cidadã, com relação a diferentes temas que

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

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.

tomaram visibilidade, como a difusão de DRM (2008), o voto eletrônico (2009 e 2016), o reconhecimento facial e, mais recentemente, a inteligência artificial.

Trata-se de fato da única organização que impulsionou uma tarefa de difusão sistemática de fôlego sobre esses temas por meio de notas de imprensa regulares em diferentes meios.[8] Ainda que não tenham se dedicado expressamente à difusão do uso de ferramentas de criptografia das comunicações contribuiu para gerar uma série de discussões mediante textos e autores que, em geral, acompanhavam o uso das ferramentas criptográficas mencionadas.

Provavelmente uma das características particulares do contexto local foi a precoce criação de uma revista autogestiva fortemente política como *En defensa del software libre* [Em defesa do software livre] na Buenos Aires de 2010. Mesmo que sua rádio de repercussão tenha sido reduzida, tratou-se da tarefa de introdução de uma agenda própria de discussões e autores que buscava uma politização inexistente no país.

Além de Richard Atallman — convidado para vir à Argentina pela Fundación Vía Libre em duas ocasiões — autores como Dmytri Kleiner, Eben Moglen, Maxigas, Evgeny Morozov, Johan Söderberg, Jakob Rigi y Michel Bauwen eram apresentados pela primeira vez na Argentina, tanto a partir das páginas da revista como de sua coleção editorial.[9]

A diferença específica desse projeto residia no vínculo direto a uma cultura autônoma das esquerdas, que promoviam uma agenda centrada em licenças *copyfarleft* (e não *copyleft*),[10] plataformas digitais horizontais e anti-hierárquicas (como a Loomio) e uma reflexão baseada nas possibilidades da produção de pares, inclusive antes da criação da revista específica sobre o tema, *Peer production* (Países Baixos, 2012), onde avaliavam a promessa do p2p de um novo modo de organização do trabalho e sua produção.

Além disso, a partir daí, foram promovidas oficinas dedicadas especialmente à difusão de OTR, GnuPG e TOR com uma leitura política dessas ferramentas, junto com a criação de oficinas de instalação de GNU/Linux e ferramentas de segurança como Iptables.

Esses últimos projetos estiveram vinculados à trajetória local do *Partido Interdimencional Pirata* (PIP) organizado na Argentina também desde o ano de 2010. Iniciados quatro anos antes no norte da Europa, os partidos pirata promoveram sobretudo uma agenda de direitos civis, democracia direta, cultura livre, privacidade da informação, transparência da informação, liberdade de expressão e neutralidade da rede.[11]

Por outro lado, entre 2014 e o 2017, a experiência local alcançou em seu momento de maior visibilidade em torno de 200 membrxs, durante os anos em que também ofereceram oficinas de criptografia chamados Grog & Tor e conversas e cursos sobre privacidade e gênero, ao mesmo tempo em que desenvolveram a coleção editorial Utopia Pirata. O número de suas publicações já supera 30 títulos – com uma dúzia de títulos como livros e folhetos longos.

---

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

Além disso, há alguns textos programáticos para organizar-se horizontalmente, essa coleção introduz autores como David Graeber, Johan Söderberg, Rick Falkvinge, Gabriella Coleman, Starhawk, Amador Fernández-Savater e Aaron Swartz, enquanto retomam para sua agenda autorxs como Oscar Varsavsky, Murray Bookchin e Hakim Bey.[12]

Sobretudo nos últimos quinze anos, existiram na Argentina diferentes projetos vinculados à conformação de redes libres de topologia de malha (mesh). Baseados em software livre, seu objetivo geral consiste em desdobrar redes livres comunitárias de baixo custo, em muitos casos em zonas de difícil acessibilidade a serviços digitais. Apesar de os projetos mais recentes terem sido acompanhados por diferentes ONGs, desde 2002, houve projetos de diferentes graus de sucesso em Rosario, Mendoza, Córdoba, Buenos Aires e no delta do rio Tigre.

No caso do projeto *Buenos Aires Libre* (2006), seu principal objetivo foi conseguir que a interconexão descentralizada deixasse de depender exclusivamente das grandes empresas. Ainda que muitas delas se encontrem hoje em dia descontinuadas, seguem sendo uma opção para espaços de difícil acesso.[13] Mais uma vez, a importância desses empreendimentos coletivos torna-se primordial, altamente produtiva, no momento de gerar comunidade e discussões a respeito de uma internet anti-hierárquica, livre, independente e crítica da centralização dos serviços. De todo modo, as ferramentas criptográficas mencionadas como eixo deste informe não fazem parte de seus programas. Hoje em dia, trata-se de projetos promovidos sobretudo pela Libre Router e Alter Mundi com publicações sobre o tema.[14]

Como em todo o mundo, o movimento ao redor do software livre gerou não apenas grupos de suporte, mas ativistas, entusiastas, cooperativas de trabalho, militâncias, organizações, grupos de contato em diferentes redes sociais e canais de mensageria e conferências. Nesse sentido, só alguns permaneceram promovendo uma agenda cultural ao longo do tempo.

Entre as conferências, cabe destacar o evento anual chamado *Festival Latinoamericano de Instalación del Software Libre* (FLISOL) [Festival Latino-americano de Instalação de Software Livre] que, por meio de seus programas, em cada uma de suas edições, tornou-se em espaço de muitas oficinas vinculadas à criptografia e à privacidade, por exemplo: sobre a utilização de servidores próprios, o funcionamento e o uso de TOR e OTR, a propagação de serviços de mensageria federados e autônomos, a importância de usar essas ferramentas, entre outros.[15] Em menor escala, algumas cooperativas de trabalho de desenvolvimento de software deram lugar a oficinas sobre comunicações seguras.[16]

Ao falar de *hacklabs* e *hackerspaces*, partimos da diferenciação feita por Maxigas,[17] quem propôs pensá-los como duas genealogias. Segundo esse texto os chamados *hackerspaces* se relacionam a uma tradição californiana, com espaços neoliberais de discussão e inovação tecnológica financiados por grandes empresas. Enquanto os hacklabs se organizariam sob uma cultura autonomista e autogestionária. Para o caso argentino, ou melhor, para

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 Consultarlos programas das últimas edições: https://flisol.info/

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

17 Maxigas [seud.] (2015). Hacklabs y Hackerspaces: rastreando duas genealogias. En Defensa del Software Libre 3. https://endefensadelsl.org/hacklabs-y-hackerspaces.html

as pessoas de Buenos Aires, essa distinção acaba sendo muito adequada e, de fato, os três hacklabs que funcionaram e funcionam foram espaços a partir dos quais, de diferentes formas, difundiu-se o uso de criptografia para as comunicações pessoais.

O hacklab de Barracas funcionou entre 2012 e 2016, com membrxs vinculadxs tanto ao Partido Pirata da Argentina (PIP) como a publicação *En defensa do software livre* (EDSL). Na mesma direção, foi um dos poucos espaços que organizou cryptoparties, ou seja, eventos destinados a trocar e consolidar as respectivas chaves públicas GnuPG em conjunção com outras oficinas de segurança. Depois do seu fechamento, algunxs de seus membrxs formaram o hacklab Rlyeh em 2017 sem a participação do Partido Pirata local.[18] Além disso, entre 2012 e 2017 existiu um hacklab menos ativo na cidade de Mar del Plata.[19]

O Centro cultural Terra Violeta, vinculado à Rede Argentina de Gênero, Ciência e Tecnologia (RAGCYT) fundada em 2011, foi outro espaço especialmente aberto a oficinas sobre gênero, tecnologia, defesa digital e ferramentas de criptografia. Pelo menos desde 2012 houve aqui várias oficinas feministas de autodefesa digital.[20] Além disso, entre 2016 e 2019 mensalmente ocorreu o evento Hacklab Violeta o *Grog & Torta*, definido como uma "oficina feminista de autodefesa digital" e também apoiado pelo PIP.

Fora do circuito mencionado até agora, os livros e autorxs que circularam com certa repercussão pertencem a um espectro mais amplo que pode ser considerado comum ao âmbito internacional. A tradução de *Cypherpunks* — de Julian Assange, Jacob Appelbaum, Andy Müller-Maguhn e Jéremie Zimmermann — foi publicada em 2013, apenas um ano depois da publicação da versão original em inglês, assim como aconteceu com *Cuando Google conoció Wikileaks.*[21]

Além da introdução-manifesto a favor de "armas" criptográficas, a edição em espanhol acabou ficando mais interessante por conter uma nota crítica não apenas à vigilância estatal, ao PRISM e sua ligação com a NSA, mas sobretudo à vigilância empresarial sobre o PRISM. Contudo, o livro careceu de maiores repercussões locais, que ficaram quase totalmente a cargo do jornalista Santiago O'Donnell. Após revelações de Snowden, algumas discussões pareciam tomar um novo fôlego, mas isso não se traduziu em nível global em aumento do uso da criptografia.[22]

Podemos pensar que o circuito descrito foi também o que recuperou na Argentina suas repercussões. Nesse âmbito, as jornalistas que abordaram assuntos relacionados nos anos posteriores foram Natalia Zuazo[23] e Marta Peirano.[24] Entre eles, só o último livro com prólogo de Snowden se propunha confeccionar uma "introdução à criptografia para redações, whistleblowers, ativistas, dissidentes e pessoas humanas em geral": argumentando a favor do uso dessas ferramentas.

---

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.

Dentro do espectro relacionado aos livros, publicistas e ativistas, outro eixo a considerar no momento é de visitantes estrangeirxs. Entre elxs, Richard Stallman, Jéremie Zimmerman, Marta Peirano e Renata Ávila visitaram a Argentina nos anos abordados, no geral com convites ligados aos grupos associações e hacklabs já mencionados.

Finalmente, mencionaremos algumas editoras que deram a conhecer uma série de textos sobre esses debates com uma proposta de intervenção mais teórica. Nesse sentido, a editora Heckt editou uma precoce compilação de textos sobre ativismos digitais[25] e as traduções dos textos dos coletivos Tiggun[26] e Comitê Invisível,[27] com aproximações à cibernética a partir da filosofia francesa. Em um sentido mais amplo, a editora Caja Negra desenvolve desde 2014 uma bem-sucedida coleção sobre novas tecnologias e políticas, traduzindo autores como Mark Fisher, Éric Sadin, Byung-Chul Han e Nick Srnicek, entre otrxs.

Nessa direção, o âmbito acadêmico interessado pelas esquerdas foca sobretudo nas perspectivas aceleracionistas ou na teoria crítica da tecnologia[28] em torno da revista Redes: revista de ciências sociais, ciência e tecnologia (Bernal, 1997). O único evento acadêmico dedicado especificamente a essas problemáticas com um impulso de difusão foi o realizado pela rede de estudos sobre vigilância *Lavits* (*Latin American Network of Surveillance, Technology and Society Studies*), que se fundou em 2009 dentro da PUCPR- Pontifícia Universidade Católica do Paraná (Curitiba, Brasil) e em 2017 celebrou seu encontro em Buenos Aires.

De configuração mais recente, em 2019 criou-se o *Observatorio de Derecho Informático Argentino* (ODIA), orientado a problemáticas legais vinculadas à informática, que, nesses últimos anos realizaram ações em torno dos programas de reconhecimento facial, o sistema de gestão dos casos judiciais utilizado no país e a aplicação oficial utilizada aqui.[29] Sem tampouco ter uma ligação direta com a difusão de ferramentas pessoais de criptografia, também nos últimos anos adquiriu visibilidade Cybercirujas e sua revista *Replay*, dedicada à recuperação de equipamentos contra a obsolescência programada.[30]

Não vinculadas ao ambiente acadêmico, mas mais no sentido técnico e profissional, podemos destacar as duas conferências de segurança informática Ekoparty (iniciadas em 2002) e NotPinkCon, destinada a incrementar o interesse das mulheres e dissidências pela segurança informática. Ao se tratar de eventos técnicos, também não se conformaram como um espaço de difusão da criptografia em nível pessoal.

• Conclusão

Em resumo, em boa medida, existe uma difusão ampla do software livre, discussões de licença por meio de diferentes tipos de comunidade, assim como de segurança ou uma discussão acadêmica sobre tecnologia sem que isso implique necessariamente uma difusão

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

29 https://odia.legal/

30 https://revistareplay.com.ar/

de ferramentas criptográficas. Provavelmente uma revisão das agrupações que

impulsionaram discussões e usos das mencionadas ferramentas criptográficas alcance apenas um panorama parcial sobre a situação na Argentina. Ao se centrar nas publicações locais e deixar de lado comunidades digitais internacionais, essa perspectiva obtém seus próprios limites. No entanto, a partir do trajeto realizado, as seguintes considerações finais podem ser propostas para o debate.

• Recomendações

• Em primeiro lugar, fica claro que as discussões sobre a necessidade pessoal de criptografia não circulam isoladas, mas junto com outra serie de preocupações comuns que podem ser organizadas nos seguintes eixos.

(i) Privacidade da informação: em boa medida cristalizado em nível global por meio da importância da intencionalidade que tomaram os casos Wikileaks, Assange, Maning, Snowden e Cambridge Analytics.[31]

(ii) A discussão pelas licenças, o acesso ao conhecimento e aos direitos de propriedade intelectual a partir dos novos modos de circulação dos bens culturais: um debate iniciado pelo software livre na década de oitenta, mas que obteve repercussão em torno das discussões pelas leis conhecidas como o uso do p2p para as trocas de música e de filmes e o impulso das leis PIPA e SOPA nos Estados Unidos (sobretudo entre 2011 e 2012) (Ariño, 2019).

(iii) Em menor escala, o otimismo do Software Livre e o p2p como modos de produção e difusão em direção a uma nova organização do trabalho[32];

(iv) e a chamada governança de internet levada a cabo por diferentes organizações para o estabelecimento comuns de padrões.[33]

• No entanto, nesse último ponto se faz necessário promover uma diferenciação. Tanto em nível internacional como local, as publicações destacadas mostram que os assuntos ligados à governança circularam separadamente, e os grupos ativistas que mais impulsionaram o uso da criptografia são céticos sobre qualquer tipo de regulação, de modo que a única solução é implementar criptografia em nível pessoal (isso pode ser visto claramente em Assange et. al., 2013, ou em nível local nas publicações do Partido Pirata.)

• Como acontece em muitos campos vinculados à tecnologia, trata-se de um campo hegemonizado por homens cis, tanto em nível local como internacional.[34] Contudo, se pode pensar também que os grupos ativistas mais autonomistas se mostraram especialmente abertos a discussões e críticas em torno do gênero.[35]

---

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

32 Domínguez Rubio, 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, dosky.

35 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

• Em nível local, os dados com que contamos e as plataformas de difusão identificadas falam de um espaço de circulação reduzido centralizado em Buenos Aires, com escassas referências a cidades de Rosario, Córdoba e Mar del Plata. Em nível regional, o recorte desse informe que parte de um "nacionalismo metodológico" deixa de lado algumas organizações de alcance regional com publicações que difundiram assuntos vizinhos; como, por exemplo, a *Alianza para el cifrado de América Latina y el Caribe* (AC-LAC), fundada recentemente em 2021 com uma agenda específica sobre o criptografia[36]; ou a *Asociación para el Progreso de las Comunicaciones* (APC) fundada já em 1990 com um alcance regional[37]; ou *Direitos Digitales*, fundada no Chile em 2004, de onde se realizaram suas publicações, e que alcançou um alcance regional nos últimos anos.

• Por último, o segundo limite desse informe reside no seu enfoque nas publicações realizadas sobre criptografia. Isso deixa fora uma importante quantidade de oficinas de segurança realizados por ativistas em risco, tanto na Argentina como em outros países. Trata-se de informação que não é pública e funciona por canais delimitados, no entanto, constituindo-se como um modo fundamental da difusão das ferramentas de criptografia: para ativistas feministas a favor do aborto, comunidades indígenas do norte e do sul do país e movimentos camponeses. Rastrear unicamente o que foi publicado tem esse limite. De mesmo modo, também não se trata de uma abordagem útil para atender urgências de militância de segurança física, Em um contexto de fortes necessidades e de conflito, falar de criptografia ainda parece um passo muito distante. Antes disso, por exemplo, é importante trabalhar a exposição nas redes sociais.

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.

Organização: Instituto de Referencia em Internet e Sociedade

Políticas públicas e mobilizações sociais sobre criptografias no Brasil

• Introdução

No Brasil, algumas normas vigentes tangenciam a criptografia: Marco Civil da Internet e respectivo decreto regulamentador, Lei Geral de Proteção de Dados, Estratégia Nacional de Segurança Cibernética e Política Nacional de Segurança da Informação. Embora elas não protejam expressamente o uso da criptografia, a ausência de proibição implica sua autorização legal.

Ameaçando esse cenário, propostas legislativas pretendem impor a provedores de serviços criptografados obrigações de monitoramento, decifragem ou custódia de chaves. Em contraponto a tais perigos, iniciativas da sociedade civil para a defesa, manutenção e difusão social de uma criptografia forte no Brasil demonstram a importância de mobilizações de resistência, e apresentam um campo mais crítico às iniciativas normativas para limitar o uso livre ou mesmo quebrar a criptografia.

No somatório, a despeito de algumas graves situações de constrangimento ou questionamento, persiste no arcabouço normativo e jurisprudencial brasileiro o apoio ao uso da criptografia, mesmo sem garantia explícita, com respaldo das organizações da sociedade civil.

Essa publicação tem como objetivo apresentar a complexa situação atual das políticas públicas e das mobilizações sociais sobre a criptografia no Brasil, oferecendo um panorama da legislação vigente, projetos de lei, processos judiciais, e campanhas de mobilização social, além de um diagnóstico de riscos e ameaças ao pleno exercício de direitos humanos pertinentes: liberdades de expressão, de opinião, de manifestação e de associação, privacidade, segurança, e proteção de dados pessoais.

• Metodologia

A metodologia utilizada se baseou, em busca de confiabilidade e densidade teórica, na revisão sistemática da literatura pertinente, com recorte empírico em obras selecionadas e avaliadas mediante critérios e procedimentos explícitos e organizados, perpassando pelo mapeamento do estado da arte sobre a situação legislativa e jurisprudencial da criptografia no Brasil, além das mobilizações civis na área. Para uma averiguação da bibliografia realizou-se um mapeamento de obras relevantes que foram utilizadas como pontos centrais no

relatório desenvolvido.

No âmbito legal, analisamos as principais normas vigentes com aproximação ao tema, mapeando proteções jurídicas, autorizações legais de uso e possíveis margens para ações de ameaças. A partir desse esquema, foi possível diagnosticar as propostas legislativas e processos judiciais que analisam atos repressivos estatais para quebra de criptografia e acesso a dados pessoais: a reforma do Código de Processo Penal prevê a possibilidade de interceptação telemática; o PL 2518/2019 impõe o monitoramento ativo; o PL 2630/2020 exige a rastreabilidade de comunicações, mesmo que cifradas; entre outros projetos de lei. Ainda, no Supremo Tribunal Federal, a quem cabe definir a interpretação da Constituição Federal, há risco de o Poder Judiciário legitimar a quebra da criptografia nas ações sobre bloqueios do WhatsApp (ADI 5527 e ADPF 403) e o acesso de autoridades policiais a dispositivos móveis durante flagrante (Tema de Repercussão Geral nº 977), para averiguação da vida íntima e privada e acesso a dados pessoais, permitindo investigações repressivas, sem garantias legais e constitucionais.

Por fim, mapeamos as formas insurgentes da sociedade civil frente às ameaças analisadas. A Coalizão Direitos na Rede organiza a criptoAgosto desde 2020, conclamando o reconhecimento da ampla importância da criptografia. Também emergiram as criptoFestas: iniciativas descentralizadas, difundidas pelo mundo a partir da Austrália. Várias edições no Brasil constituíram espaços de *artivisimo*, unindo cultura, tecnologia e política: CryptoRave em São Paulo, CriptoJP na Paraíba, CriptoBaião no Ceará, CriptoTrem em Minas Gerais, e CriptoFesta em Pernambuco. Ainda, há esforços internacionais, como o Dia Global da Criptografia e a organização da Aliança para Criptografia na América Latina e Caribe.

Desse modo, a metodologia adotada cria um escopo analítico jurídico e institucional, a partir de bibliografias relevantes, que apresenta o campo da criptografia no Brasil, com um olhar crítico para as evidências e orientando investigações futuras.

• Contexto e antecedentes

As tentativas estatais e privadas de contorno refletem uma complexa disputa mundial sobre criptografia, objeto de várias considerações por órgãos de defesa de direitos humanos. Em contextos bélicos, o seu valor informacional oferece proteção às táticas militares, beneficiando o poder público; mas ao proteger a privacidade de particulares, ela é vista como um risco ao Estado (notadamente em regimes totalitários, onde a busca por aplicações criptografadas tende a aumentar).[38]

Dessa contraposição de perspectivas surgiram as chamadas *CryptoWars (*Guerras Criptográficas*):* embates entre sociedade civil e Estado, em torno da demanda por acesso excepcional de autoridades a portas clandestinas, a pretexto de afastar os riscos da criptografia para a segurança pública, e, por outro lado, a demanda no mercado da privacidade pela elevação da segurança criptográfica em produtos comerciais. O conflito tem questões perenes, ainda sob disputa jurídica, tecnológica e argumentativa. Mas, historicamente, dois períodos são marcantes: o final do século XX e o ano de 2013, reconhecidos por parte da literatura como primeira e segunda guerras criptográficas.[39]

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.

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.

A primeira *CriptoWars* começa no contexto da II Guerra Mundial. Reduzindo a criptografia ao seu potencial militar, os EUA tencionaram para restringir o seu uso fora e dentro do país, impondo barreiras à exportação de tecnologias mais avançadas, e coibindo pela NSA a difusão doméstica.[40] A segunda possui três eventos notórios. Em 2013, as denúncias de Edward Snowden, ex-integrante da CIA e da NSA, sobre práticas de cibervigilância dos EUA[41] contra indivíduos e chefes de Estado -.

Por fim, o último evento se refere ao caso Apple vs FBI, em 2015[42], em que a autoridade investigativa buscou obrigar a empresa a contornar a criptografia e fornecer acesso ao iPhone de um terrorista morto, sob a alegação de segurança nacional. O debate público efervesceu, acirrando a disputa narrativa antagônica entre criptografia e segurança pública.

No contexto brasileiro, esse conflito tomou forma em disputas judiciais envolvendo o WhatsApp, entre 2015 e 2016, quando a empresa resistiu a fornecer acesso a dados de usuários.[43] Foram ajuizadas no Supremo Tribunal Federal duas ações de controle concentrado de constitucionalidade, para "questionar a validade jurídica das ordens de bloqueio do WhatsApp perante a instância máxima do Poder Judiciário brasileiro, para que a decisão crie um mecanismo jurisprudencial que impeça novas ordens de bloqueio da plataforma".[44]

Assim, tanto quanto EUA, Europa, Índia e outros países que vivenciam conflitos em torno da criptografia, o Brasil faz sua disputa no contexto judicial e político, com um papel ativo, inclusive da sociedade civil, como veremos a seguir.

• Políticas públicas e mobilizações sociais sobre criptografias no Brasil

• A situação normativa da criptografia no Brasil

A utilização da criptografia como meio central para garantia da segurança no meio digital tem se ampliado nas últimas décadas.[45] Todavia, as controvérsias ao seu uso circunscrevem o campo. Instituições de persecução penal explicitam a dificuldade investigativa pela criptografia, o que chamam de "obscuridade" (*Going dark*), o que tornaria as comunicações digitais indecifráveis para as autoridades policiais.

No Brasil, algumas normas arejam o tema da criptografia, e tangenciam, de alguma forma, sua importância como técnico de salvaguarda à integridade, confidencialidade, autenticidade e disponibilidade de dados digitais. O princípio da segurança – previsto

---

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.

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.

principiologicamente no Marco Civil da Internet[46] ao lado de outros direitos humanos pertinentes como cidadania, livre expressão, privacidade, proteção de dados pessoais etc. – se densifica no decreto regulamentador[47] com o dever de os provedores garantirem inviolabilidade de dados via "encriptação ou medidas de proteção equivalentes".

A Lei Geral de Proteção de Dados,[48] a título exemplificativo, pautada pela construção de toda uma cultura jurídica de salvaguarda, ao tratar de sigilo e segurança exige "técnicas adequadas que tornem os dados pessoais afetados ininteligíveis (...) para terceiros não autorizados a acessá-los".

A Estratégia Nacional de Segurança Cibernética[49] recomenda soluções de criptografia para fortalecer a governança; o uso social generalizado de recursos criptográficos para comunicação segura de assuntos sensíveis; e o desenvolvimento de competências e soluções em criptografia para incentivar pesquisa e inovação. E a Política Nacional de Segurança da Informação[50] delega à alta administração dos órgãos e entidades da administração pública federal o papel de orientar programas, de projetos e de processos para "a utilização de recursos criptográficos adequados aos graus de sigilo exigidos"

Nenhuma das normas vigentes prevê expressamente o direito ou a proibição de um livre uso da criptografia. Por um lado, a ausência de vedação implica permissão legal, à luz do princípio da autonomia da vontade privada, cabível para pessoas físicas e jurídicas. Mas, por outro lado, fica aberto o espaço para diversos tipos de abusos e excessos, que ameaçam ou restringem essa liberdade.

• Ameaças à criptografia no Brasil

No âmbito privado, os recorrentes vazamentos de dados pessoais ilustram um dos riscos de a proteção por criptografia ainda depender da escolha de empresas, diante da incapacidade prática de qualquer fiscalização pela Autoridade Nacional de Proteção de Dados; e no âmbito estatal, os problemas podem ser identificados nos três poderes.

No Executivo, sem iniciativas propositivas, como ações educacionais formais voltadas para a promoção do tema, a violação ocorre na própria política de segurança pública. Empregam-se técnicas de investigação, sem mínimos critérios legais objetivos, banalizando diversas práticas inadequadas, desde a vulgar "criptoanálise de mangueira de borracha"[51] até

---

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.htm

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.htm

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.htm

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.htm

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 nacional.). 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.htm

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-man-gueira-de-borracha/

o sofisticado hacking governamental.[52]

No Legislativo, entre muitas propostas normativas,[53] a reforma do Código de Processo Penal[54] pode regular meios para interceptação telemática; o projeto de lei nº 2.518/2019 pode prever mecanismo para monitoramento ativo de alvos; e a versão do projeto de lei nº 2.630 de 2020 aprovada no Senado cria para aplicativos de mensagens instantâneas a obrigação de "rastreabilidade de comunicações".[55]

No Judiciário, cabe ao Supremo Tribunal Federal apreciar a constitucionalidade do bloqueio do WhatsApp, tendo como eixo a exigibilidade de a empresa abandonar padrões criptográficos de segurança para viabilizar o acesso investigativo a dados de seus usuários. Os votos já proferidos na ADPF nº 403,[56] pelo Ministro Edson Fachin, e na ADI nº 5527,[57] pela Ministra Rosa Weber, protegem a criptografia. O julgamento está suspenso desde maio de 2020, sem garantias de que não será legitimada a quebra da criptografia. Ademais, cabe à Corte analisar a validade da prova produzida durante inquérito policial mediante acesso, durante flagrantes, sem autorização judicial, a dados em telefone celular, relacionados ao delito e hábeis a identificar o agente, conforme o Tema de Repercussão Geral nº 977[58] (ARE 1042075).[59]

Esse cenário abre possibilidades de arbitrariedades na averiguação da vida íntima e privada e no acesso indevido a dados de quaisquer pessoas, com especial prejuízo para segmentos populacionais mais vulneráveis, vítimas habituais de investigações repressivas, sem efetivas garantias legais e constitucionais.

• Iniciativas da sociedade civil para a defesa, manutenção e difusão social de uma criptografia forte no Brasil

Frente aos desafios, a sociedade civil assume um papel ativo nessa disputa. Pesquisadores, ativistas, coletivos e organizações não governamentais, tomam a dianteira da defesa da criptografia no Brasil e ao redor do mundo. Nesta seção do relatório, nos debruçamos sobre ações pautadas pela sociedade civil brasileira com o intuito de frear as ameaças a criptografia forte.

---

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-investiga-coes-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

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 identificar 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 telefo-nia celular relacionado à conduta delitiva, hábeis a identificar o agente do crime.). https://portal.stf.jus.br/jurisprudenciaRepercussao/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

A ADPF nº 403 e a ADI nº 5527 são demonstrativos dessa dianteira, apesar do caráter constitucional de tais ações exigirem determinadas condições para figurar no polo ativo da proposição, a sociedade civil se fez presente nas audiências públicas, e participou ativamente do processo como *amicus curiae*. Além de intervenções judiciais, as várias frentes ocupadas pelos movimentos pró-criptografia, ampliam a capilaridade em espaços que vão desde a difusão do papel da criptografia nas rotinas humanas, até o advocacy em políticas públicas.

As Criptofestas são um exemplo das possibilidades reinventadas pela sociedade civil para articular e difundir uma cultura criptográfica. Seu surgimento é datado em 2012, na Austrália, como resposta a aprovação de um projeto de Emenda legislativa para cibercrimes, que condicionalizava a retenção dos dados do usuário por dois anos[60].

A proposta da festa surge com alguns princípios norteadores: a) a descentralidade, a organização deve ser aberta, sem enviesamentos de poder; b) ser um espaço de troca, assim, a participação não deve ser condicionalizada a ter um conhecimento prévio sobre criptografia, mas ao desejo de aprender e trocar experiências; c) colocar a mão na massa e testar, por ser um espaço de autogestão, é preciso que todos colaborem, independente do seu nível de confiança ou habilidades, a construção é coletiva; d) independência político e comercial, apesar de ser um espaço político, não é saudável que se vincule a partidos políticos e nem empresas ou ONGs, pois esse envolvimento pode reduzir o respeito aos outros princípios; e) as ferramentas recomendadas devem ser de acesso gratuito ou aberto, para evitar intervenções econômicas; f) tolerância zero a assédios e violências, sejam físicas ou verbais.[61]

Por seu caráter descentralizado, as Cryptofestas se difundiram pelo mundo, inclusive no Brasil. É preciso registrar, que por esse mesmo motivo, não há de forma sistematizada dados sobre todas as festas já organizadas, o que se apresenta como um desafio a essa pesquisa. O site da Cryptoparty[62] possui o registro de 6 festas no Brasil, sendo elas, a CriptoTrem, realizada em Belo Horizonte, 2019; a CriptoRave de São Paulo, realizada anualmente; a CryptoFesta Taubaté, realizada em 2017; a CriptoFesta Recife, realizada em 2018, na capital Pernambucana; a nanoCRYPTOFesta Tarrafa, realizada em 2018, na cidade de Florianópolis; e o Criptobaile, realizado em 2018, no Distrito Federal. É preciso destacar a existência de outras Cryptoparty que não estão correlacionadas no site, como exemplo temos a CriptoFunk no Rio de Janeiro,[63] e a CriptoJP na Paraíba, a CriptoBaião no Ceará.[64]

Outra forma de articulação da sociedade civil no Brasil, é a promoção de coalizões, frentes que reúnem diversas pessoas e instituições, como a Coalizão Direito nas Redes - CDR[65], uma rede com mais de 50 organizações acadêmicas e da sociedade civil, que pauta, entre outras coisas, a defesa de uma criptografia forte. A CDR propôs em 2020, o lançamento do CriptoAgosto,[66] inspirada em outras iniciativas como o Dia da Internet Segura, no mês de fevereiro, nas articulações da Global Encryption Coalition, e nas já mencionadas CryptoFestas. Desde então as organizações participantes da Coalizão, tem se empenhado em desenvolver ações e projetos no mês de agosto, que demarquem a importância da criptografia e sua defesa.

---

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

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/

Outra agenda construída pela sociedade civil, é a articulação de uma Aliança latino-americana e caribenha pela defesa da criptografia, a AC-LAC. Criada pela junção de 23 organizações de diversos países da América Latina e Caribe, com a missão de produzir uma plataforma coletiva que amplie o conhecimento sobre criptografia como direitos fundamentais e humano, além de articular esforços transnacionais para trocas e mobilizações em defesa da criptografia, avançando assim com uma agenda pró-ativa.[67]

Assim, as organizações da sociedade civil brasileira assumem protagonismo na defesa de uma agenda pró-criptografia, na busca de refrear os avanços das ameaças a uma criptografia forte.

• Conclusão

No universo de diferentes ameaças e prejuízos que o poder público impõe a direitos humanos envolvendo a criptografia decorrem, em alguma medida, do pressuposto equivocado de haver uma contraposição inconciliável entre proteção de dados digitais e segurança pública. Desde a primeira criptoguerra até as práticas de hacking governamental pelo governo brasileiro, Estados de todo o mundo não parecem compreender institucionalmente a importância da criptografia forte para o próprio interesse público, em diversas dimensões. Os riscos identificados no Brasil demandam soluções específicas e locais, mas devem ser encarados como parte de um complexo problema global, que também evoca cuidados internacionais, com a cooperação entre países.

Para além da liberdade de expressão e da privacidade, limitam-se uma série de outros direitos fundamentais aos seres humanos quando práticas governamentais não apenas chancelam como incentivam abusos, excessos e omissões por parte de empresas privadas que se colocam na condição tecnológica e econômica de tutoras da cibersegurança de grande parte da população que se vale dos recursos da sociedade da informação sem capacidade para avaliar pessoalmente a confiança do funcionamento de seus dispositivos e sistemas e redes digitais.

Mas, conforme o recente relatório do Conselho de Direitos Humanos da ONU, os repetidos esforços demonstrativos de beneficiários da criptografia, de grupos vulneráveis a setores estratégicos, não se mostraram suficientes para reduzir esses perigos. Além de renovarem-se as recomendações para empresas e governos, faz-se premente a assunção de compromissos comuns na comunidade internacional, para que as soluções e avanços na proteção, defesa e promoção da criptografia forte sejam alcançadas de modo consistente e harmônico em todos os países.

• Recomendações

A partir do cenário diagnosticado, sugerem-se os seguintes passos de incidência para as organizações da sociedade civil, tendo em vista a promoção, defesa e proteção dos direitos humanos relacionados à regulação da criptografia no Brasil:

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

- Atuar junto ao Poder Legislativo para:

    a. apontar, nos projetos de lei em geral, os riscos de iniciativas normativas que estipulem restrições diretas ou indiretas, gerais e indiscriminadas sobre o uso da criptografia, prevendo, por exemplo, proibições, criminalização, imposição de padrões de criptografia fracos ou requisitos para verificação geral obrigatória do lado do cliente;

    b. apontar, nos debates do Novo Código de Processo Penal e da Lei Geral de Proteção de Dados em Investigações Criminais e Segurança Pública, que a interferência na encriptação de comunicações privadas de particulares só deva ser efetuada quando autorizada por órgão judiciário independente e caso a caso, tendo como alvo indivíduos se for estritamente necessário para a investigação de crimes graves, ou para a prevenção de crimes graves, ou ameaças à segurança pública ou à segurança nacional;

    c. estimular uma agenda positiva para promover e proteger a criptografia forte, por meio de debates, eventos, seminários e audiências públicas.

- Atuar junto ao Poder Judiciário para:

    a. acompanhar o desenvolvimento das ações de controle concentrado de constitucionalidade (ADI 5527 e ADPF 403), avaliando a oportunidade e conveniência de se solicitarem audiências em gabinete com os (as) Ministros (as) do Supremo Tribunal Federal;

    b. acompanhar o desenvolvimento do ARE 1042075, avaliando a oportunidade e conveniência de se solicitar audiência em gabinete com o Ministro Relator, Dias Tóffoli, bem como com demais integrantes da Corte;

- Atuar junto ao Poder Executivo para:

    a. fortalecer a supervisão institucional e o monitoramento social das atividades de contratação de hacking governamental;

    b. chamar a atenção da opinião pública sobre atividades abusivas, a exemplo da criptoanálise de mangueira de borracha;

    c. estimular uma agenda positiva para promover e proteger a criptografia forte, por meio de debates, eventos, seminários e audiências públicas.

- No âmbito das organizações da sociedade civil, promover eventos de debate sobre a temática, envolvendo especialmente as organizações ligadas agendas como:

    a. *amici curiae* na ADI 5527 e ADPF 403;

    b. integrantes da AC-LAC;

    c. organizadoras de eventos de difusão, 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

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

O uso da criptografia como um mecanismo de combate à vigilância estatal e a proteção de garantias e direitos fundamentais – uma avaliação sócio-legal da proposta regulatória chilena

• Introdução

Observando o rápido desenvolvimento das tecnologias informacionais e das telecomunicações é possível perceber que a temática da criptografia tem assumido um papel importante nas discussões e estudos acadêmicos e políticos. O presente trabalho visa analisar como a criptografia tem sido abordada no Chile, mapeando como esse tema é tratado nos mais diversos setores sociais com o objetivo de identificar indicações positivas da adoção da tecnologia, bem como os riscos a ela associados.

Desde os anos 90 que estudos e políticas são produzidos no Chile abordando a temática da cibersegurança. Em 2017, foi proposta a Política Nacional de Cibersegurança, com direcionamentos expressos à impulsão do desenvolvimento da criptografia. A partir desse período, o Chile passou por um processo particular de amadurecimento legislativo da temática, com a criação de leis ao redor do tema, o crescente envolvimento da sociedade civil apontando a necessidade de incluir previsões sobre criptografia na Constituição, além do crescimento de atividades no campo da cibersegurança.

Entende-se, assim, ser coerente o estudo dessa realidade para o fortalecimento da compreensão do que tem sido produzido no contexto latinoamericano, bem como para impulsionar o estudo sobre a regulamentação da criptografia em nosso país

• Metodologia

Utilizando uma abordagem de pesquisa sociolegal orientada pelo estudo de caso, o trabalho proposto explora o objeto de estudo por meio de análise bibliográfica e documental (exame de legislações e instrumentos normativos, notícias, publicações e notas técnicas legislativas, matérias jornalísticas e demais instrumentos qualitativos). O principal

objetivo é jogar luz sobre os argumentos e racionalidades que promovem ou impedem o desenvolvimento de mecanismos regulatórios que estabeleçam a adoção da criptografia como meio de proteção dos direitos digitais e de combate à vigilância digital.

• Contexto e antecedentes

Segundo relatório produzido pela Organização das Nações Unidas - ONU (2022), o Chile é o segundo país da América Latina mais avançado em termos de governo eletrônico. Todavia, a afirmação deve ser lida com moderação diante do contexto sociopolítico vivenciado pelo país especialmente no que tange a ao cenário legislativo, como se debaterá a seguir.

No Chile, as discussões referentes à cibersegurança não são recentes, haja vista que desde o ano de 1999 o país fomenta estudos sobre essa questão e, desde então, já produziu pelo menos cinco instrumentos de planejamento (*"Chile: Hacia la sociedad de la informacion"; "Agenda Digital: Te acerca al futuro"; "Estratégia Digital"; "Agenda Digital: Imagina Chile"; Agenda Digital*) que foram base para as políticas governamentais e impulsão das discussões sobre o tema.

Já no ano de 2017 foi estabelecida a Política Nacional de Cibersegurança (PNCS), contendo metas a serem alcançadas até o fim de 2022. Dentre os objetivos destacam-se: o desenvolvimento de infraestrutura preparada para enfrentar incidentes de cibersegurança; o Estado como garantidor de direitos das pessoas no ciberespaço; o desenvolvimento de uma cultura de cibersegurança por meio da educação e boas práticas; o estabelecimento de relações de cooperação de cibersegurança com outros países; bem como a participação ativa nas discussões internacionais.[68]

Especificamente no que se refere à criptografia, a PNCS reconhece o valor da tecnologia ao entender que esta permite o fornecimento de alto nível de confidencialidade e integridade para a informação, podendo ser uma possibilidade relevante para a estratégia de segurança externa do país. A partir desta compreensão, estabelece que as medidas adotadas devem promover a adoção de criptografia ponta-a-ponta para os usuários, alinhadas com os padrões internacionais, devendo ser evitado a todo custo o uso de tecnologias inseguras.[69]

Vale mencionar que a motivação dessas discussões e preocupações referente à cibersegurança, especificamente à criptografia, está especialmente relacionada com o constante desenvolvimento tecnológico, os riscos e ameaças aos direitos fundamentais das pessoas e a segurança estatal.

Como exemplo, cita-se o crescente interesse pela espionagem digital por parte dos governos da América Latina. Como aponta o relatório *Hacking Team: malware de espionaje en América Latina*, no qual é revelado que a maioria dos países da região esteve envolvida com a *Hacking Team*, empresa italiana criadora do Remote Control System (RCS), um software espião vendido a organizações governamentais ao redor do mundo.[70]

---

68 Chile (2017) Política Nacional de Ciberseguridad. [S. l.: s. n.], chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/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.] chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/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

Não é difícil compreender que vazamentos e falhas na segurança, nesse aspecto, são catastróficos. Com isso em mente, o Chile tem discutido o aprimoramento de ações em torno da temática, com enfoque na segurança da infraestrutura crítica da informação. Como será explorado a seguir, diversos setores sociais têm se empenhado na regulamentação da criptografia, estudos e estabelecimento de padrões e boas práticas.

• Avaliação do panorama chileno

O crescimento do uso e dos riscos que envolvem a sua utilização de tecnologias da informação que podem afetar não somente os direitos fundamentais das pessoas, mas também a segurança do país, fomentaram o desenvolvimento da Política Nacional de Cibersegurança do Chile.

Serve como exemplo dessa percepção a atuação da empresa "Hacking Team", que desenvolvia potentes *softwares* de espionagem, sendo a principal aplicabilidade destes a invasão de dispositivos eletrônicos e bases de dados para obter informações, tendo inclusive comercializado seus softwares com diversas agências governamentais. A lógica por trás dos *Malwares* desenvolvidos é que chama atenção: a "Violação intencional de sistemas informáticos para fazer cumprir a lei, tirando partido das suas lacunas regulamentares".[71]

Nesse contexto, o Chile adquiriu o sistema Galileo da Hacking Team, cujo nome foi modificado para Phantom, não tendo sido a aquisição feita de forma clara e transparente, já que, de acordo com Partarrieu e Jara (2015) a compra pela polícia investigativa do Chile foi feita de forma sigilosa e descoberta após o ataque informático à empresa fornecedora do software que resultou na divulgação de diversos emails.[72]

O uso de software do malware tem sua legalidade questionada, tendo em vista que a interceptação de comunicações nos países geralmente depende de ordem judicial e a tecnologia do software tem outras funcionalidades invasivas além da interceptação, como geolocalização, ativação de câmeras e microfones.[73]

Considerando o potencial invasivo dos sistemas vendidos pelo Hacking Team, há receio das consequências que a utilização de tecnologias de vigilância pode acarretar aos direitos humanos, principalmente no que tange à liberdade de expressão e direito à privacidade. Em Declaração Conjunta sobre Programas de Vigilância e seu Impacto na Liberdade de Expressão, ONU e a OEA (2013)[74] indicaram preocupação, tendo em vista que alguns Estados estavam interceptando comunicações particulares com finalidades políticas.

A criptografia, nesse contexto, seria uma alternativa protetiva relevante, já que é uma tecnologia direcionada à codificação de informações, as quais teriam sua confidencialidade preservada, tornando o conteúdo indisponível às pessoas que não têm acesso franqueado ou não estejam autorizadas a operar a decodificação.

---

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 e Jara. M. (2015). Los correos que alertaron sobre la compra del poderoso programa espía de la PDI. CIPER. 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

Destacando-se no cenário latinoamericano, sobressaindo-se na preocupação em desenvolver políticas nacionais de cibersegurança, o Chile, no âmbito legislativo, discute atualmente o Projeto de *Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información* (Boletín Nº 14.847-06). Deflagrado por iniciativa do ex-presidente da República Sebástian Piñera, a proposição foi entregue ao Senado em março de 2022.

A partir da análise da mensagem de apresentação do referido projeto de lei, infere-se a vontade política que se busca alcançar a partir dele. Observa-se a preponderância do escopo de consolidação da segurança da informação atrelada ao exercício dos direitos fundamentais por meio da administração pública digital, bem como da regulação sobre o tema junto aos particulares. Pretende-se realizar uma "guerra ao terror" cibernética, indicando medidas de prevenção a ciberataques.

A mensagem com a apresentação do PL contextualiza a criação de uma Agência Nacional de Cibersegurança que coordene o tema junto ao setor privado de forma permanente para garantir a segurança do ciberespaço, prevenindo a ocorrência de crimes informáticos e protegendo a infraestrutura de tráfego de informação.

Como aponta, busca-se viabilizar a supervigilância, estabelecendo meios para o exercício do Poder de Polícia no âmbito digital. A mensagem enviada ao Senado do Chile pela AC-LAC, Aliança para a Criptografia na América Latina e Caribe, se contrapõe a partir da garantia da proteção da criptografia no PL.[75]

Considerando o objetivo delineado na mensagem de encaminhamento do projeto de lei – com expressa menção à finalidade de supervigilância através da Agência Nacional de Cibersegurança[76], o texto normativo defere a essa instituição a competência de, em conjunto com agências de inteligência, enfrentar ameaças à infraestrutura crítica da informação e implementar ações preventivas, sem, contudo, especificar garantias mínimas aos cidadãos nesse contexto (art. 9, "l").

A opacidade do procedimento investigatório e de ações preventivas descortina o risco de quebra da privacidade permanentemente. Ademais, a ausência de multissetorialismo – com representantes expressamente endereçados à sociedade civil, à academia e ao setor privado – na composição do Conselho Técnico da Agência Nacional de Cibersegurança aponta o risco de malversação de informações e dados pessoais dos cidadãos, obtidos no escopo de um opaco sistema preventivo ao ciberterrorismo.

Infere-se que a ausência de garantia da criptografia no PL se contrapõe ao crescente movimento da sociedade civil por proteção dos direitos digitais. A autodeterminação informativa compreende a segurança e a privacidade fornecidas pela criptografia, de forma a não haver embaraços ao livre desenvolvimento da personalidade no ciberespaço.

É importante perceber que o plano de fundo para a propositura da regulação é um cenário político marcado por tensões e ensaios para uma tentativa de ruptura com a ordem constitucional herdada do governo de Augusto Pinochet. Ainda que existente uma imanente necessidade do Estado chileno em garantir a segurança da informação em suas instituições contra ameaças, ataques cibernéticos e espionagem, ante o histórico de ataques cibernéticos sofridos em tempos recentes,[77] a questão não se destaca da demanda popular

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

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. Lisboa.

por uma nova ordem constitucional. O rechaço popular pela nova Constituição Política do Chile culmina por não trazer o respaldo inerente à questão da criptografia com escopo no Projeto de Lei.

Encaminhada primeiramente ao Senado, a proposição foi debatida na *Comisión de Defensa Nacional* e na *Comisión de Seguridad Pública.* Na discussão geral do projeto, o Senador Pugh Olavarría destacou a necessidade de atualização da Política Nacional de Ciberseguridade Chilena, vigente desde 2017, requerendo prazo para indicações.

O Boletim n° 14.847-06 revela as indicações apresentadas, que envolvem supressão de expressões, incorporar novos dispositivos ou mesmo substituições, todas partindo de senadores ou do presidente da república, chancelado pelo Ministério da Fazenda, o qual apresentou Informe Financeiro Complementar aduzindo que as alterações não significariam maior gasto fiscal. O prazo para as indicações foi ampliado até o dia 22 de novembro de 2022.

No que diz respeito às disposições constitucionais, o reconhecimento do direito à privacidade, à proteção de dados pessoais e à cibersegurança estavam entre as propostas da iniciativa popular nº 57.970 feita pelo Centro de Estudios en Derecho Informático (CEDI) para que fossem mantidas e avançadas no novo texto constitucional,[78] demonstrando a demanda da sociedade civil para que tais direitos sejam protegidos com notável evolução técnico-jurídica em relação à previsão constante na constituição vigente. Destaca-se que, na iniciativa, havia menção à criptografia como forma de proteção da segurança digital.[79]

Embora não tenha sido aprovado, o texto que fora proposto para a nova Constituição chilena mostrou claro avanço em relação à garantia da cibersegurança, tendo em vista que a proposta previa regras relativas à privacidade, proteção de dados, segurança informática e promoção de direitos no âmbito digital.[80]

Em seu art.70, a proposta previa o direito à privacidade familiar, pessoal e comunitária, fazendo menção também à inviolabilidade das comunicações privadas e incluindo os metadados, indicando que "[...]3. *Toda documentación y comunicación privada es inviolable, incluyendo sus metadatos. La interceptación, la captura, la apertura, el registro o la revisión solo se podrá realizar con orden judicial previa.*",[81] limitando à vigilância estatal em relação aos dados provenientes de interações e comunicações realizadas por meio de dispositivos digitais,[82] promovendo assim a preservação de direitos dos cidadãos, bem como a continuidade da ordem jurídica.

---

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%20del%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%20del%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

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

• Conclusão

A partir da pesquisa empreendida é possível compreender o grau de complexidade da questão envolvendo a criptografia no Chile, posto que latente a discussão sobre direitos digitais nesse país. Entende-se que sob o ponto de vista legal, a tramitação do Proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información reflete a importância do tema no contexto chileno, uma vez que demonstrada a vontade legislativa em regulamentação do translado seguro de informações.

A proposta legislativa, contudo, demonstra risco de violação ao direito fundamental de privacidade, na medida em que permite uma supervigilância estatal no escopo de combate aos cibercrimes, sem o contrapeso de garantias mínimas ao cidadão.

A possibilidade de interferência de comunicações privadas, aliada à obrigatoriedade de empresas privadas compartilharem informações sobre seus usuários com a Agência Nacional de Cibersegurança representa, em outros termos, a possibilidade de estabelecimento de um estado de supervigilância permanente, viabilizando-se esta finalidade expressa na mensagem de encaminhamento do PL.

A centralização da coordenação de fiscalização e normatização em termos de cibersegurança preordena centralização de um poder ilimitado, em detrimento da inviolabilidade da comunicação. A proposta legislativa legitima ainda o uso preventivo de ações, em coordenação com agências de inteligência, sem qualquer contrapeso de proteção à privacidade do cidadão.

A criptografia se descortina como instrumento de garantia da privacidade digital, resguardando o livre desenvolvimento dos usuários de plataformas digitais. Com efeito, percebe-se a atuação dos movimentos da sociedade civil para que se faça constar a proteção da criptografia no corpo textual da propositura legislativa.

O prisma social também pôde ser observado a partir da organização da sociedade civil dada por ocasião da Proposta de Constituição Política da República do Chile, que, embora tenha sido rechaçada por voto popular, aponta para uma sistêmica e complexa organização sociolegal em prol da garantia da privacidade, da inviolabilidade da comunicação, proteção de dados e demais direitos digitais. O avanço da proteção constitucional da inviolabilidade da comunicação, e consequentemente da criptografia, restringiria o alcance da implementação do sistema de cibervigilância por intermédio de uma Lei sobre Cibersegurança no contexto chileno.

O estabelecimento de garantia à criptografia no contexto da cibersegurança nacional, caso não avance em nível legal, no texto do referido Projeto de Lei, teria consubstancia em nova fase da Política Nacional de Cibersegurança, calcado na premissa constitucional de proteção de dados e sigilo das comunicações, regulamentando a ação da Agência Nacional de Cibersegurança chilena.

A discussão política em torno do agasalho normativo da criptografia no referido projeto legislativo se relaciona diretamente com o avanço social de proteção dos direitos digitais no Chile, sendo instrumento de mensuração do grau de maturidade política no tema, servindo de base para o alcance de novas dimensões de direitos fundamentais.

• Recomendações

Uma vez observado o contexto da regulamentação da criptografia no Chile indicamos:

- Expandir a parceria realizada pela AC-LAC com outras associações civis, estendendo-se a entidades acadêmicas nacionais e latino-americanas para alcance desse objetivo;

- Criar uma campanha de conscientização massificada da comunicação, com o objetivo de alertar a população civil chilena acerca da importância da criptografia no contexto das comunicações e na proteção de direitos humanos digitais;

- Fomentar o engajamento e apoio populacional à demanda por inclusão da Criptografia no Projeto de Lei-Quadro de Cibersegurança do Chile, seja por meio de mobilização pública, inclusive digital, fortalecendo a negociação com membros das comissões do Senado em que tramita o projeto de lei com esse objetivo;

- Produzir conhecimento científico e acadêmico sobre o tema por meio da qual se apresentará uma visão holística sobre os impactos sociais da criptografia, inclusive sob o enfoque de ciências sociais e tratamento de dados estatísticos;

- Estabelecimento de um panorama concreto de viabilização de direitos digitais, correlacionando a aplicação e interpretação da atual Constituição à proteção da criptografia, através de emendas e demais mecanismos legais, dando bases para a eventual discussão de direitos digitais que devem constar na próxima Constituição Política do Chile;

- Estabelecer meios de negociação com membros do Poder Executivo para viabilizar a implementação da criptografia na regulamentação da atividade investigativa e preventiva da Agência Nacional de Cibersegurança chilena, através de nova fase da Política Nacional de Cibersegurança;

- Estabelecer um panorama de litigância estratégica em prol da criptografia no escopo de uma aliança de entidades da sociedade civil de cunho nacional no Chile, em vistas à sua garantia como direito fundamental por reconhecimento judicial.

País: Colômbia

Autor: Alejandro Moreno Baquero

Relatório do estado atual de regulação de ferramentas de criptografia na Colômbia e possíveis ações de melhora

• Introdução

Neste relatório será apresentado o estado atual das políticas públicas e das iniciativas não governamentais relacionadas ao uso, às proibições e aos direitos no campo das tecnologias de criptografia ou de encriptação na Colômbia. Também serão repassados os principais desafios e discussões no entorno colombiano com relação à regulação dessas tecnologias, incluindo as possíveis oportunidades de melhora identificadas.

O principal objetivo do presente informe é destacar as possíveis ambiguidades existentes na Colômbia em matéria normativa com relação ao uso das tecnologias de criptografia. Como elaborado aqui, a falta de transparência pode se dever principalmente a corpos normativos anacrônicos e que não respondem de forma satisfatória às necessidades atuais, especialmente em relação à proteção a grupos em condição de vulnerabilidade, tais como agentes da sociedade civil, defensores de direitos humanos, ativistas ou jornalistas.

• Metodologia

Como metodologia do presente informe, consultaram-se fontes normativas, acadêmicas, iniciativas privadas e públicas, notas jornalísticas, processos judiciais e administrativos, bem como outras fontes bibliográficas, que pudessem se referir diretamente à regulação de tecnologias de criptografia e de seus efeitos na Colômbia.

Posteriormente, como resultado dessa revisão, foram comparadas as diferentes fontes com o fim de determinar os pontos em que os desenvolvimentos normativos vigentes em matéria de criptografia encontram-se desarticulados ou se mostram insuficientes na garantia dos direitos dos cidadãos, especialmente como resultado do avanço tecnológico experimentado nas últimas décadas. Essa análise foi realizada dando atenção especial à utilidade do uso das tecnologias de criptografia para a proteção de grupos em condição de vulnerabilidade em espaços digitais, tais como defensores de direitos humanos, ativistas, jornalistas, entre outros. Dessa forma, conta com a retroalimentação da Fundación Karisma, uma das principais organizações da sociedade civil que trabalha na Colômbia pela defesa de Direitos Humanos em contextos digitais.[83]

Como comentário do autor à execução da metodologia proposta, destaca-se que, tal como se desenvolverá com mais profundidade no corpo do presente texto, os principais

83 Para conhecer mais sobre as iniciativas dessa organização, consultar: [https://web.karisma.org.co/].

desafios encontrados surgiram, precisamente, do estado ambíguo e do desenvolvimento precário que existe com relação a corpos normativos ou a iniciativas estatais aparentemente contraditórias que se referem às tecnologias de criptografia na Colômbia. Desse modo, a época em que algumas destas normas foram emitidas (por exemplo, a Lei 104 de 1993) corresponde a um contexto muito distante do atual, especialmente em matéria de uso de dispositivos eletrônicos.

• Contexto e antecedentes

Na Colômbia, a primeira referência à criptografia em um corpo normativo remonta à década de 1990, um período de importante desenvolvimento para as telecomunicações no país. Durante esse período, a Colômbia estava imersa em violência, derivada do conflito armado interno (cujos efeitos persistem) entre o governo nacional e os grupos armados, tais como as guerrilhas das FARC-EP, o ELN, as dissidências do M-19, paramilitares, cartéis de drogas e delinquência comum.

Durante essa época, paralelamente ao conflito interno, eram dados os primeiros passos no desenvolvimento das redes de Internet e as comunicações por telefone e rádio eram um elemento usado pelos diferentes atores do conflito interno para suas operações. Em consequência, como parte da estratégia para limitar a operação de grupos armados ilegais, a Lei 104 de 1993[84] incluiu uma restrição ao envio de telecomunicações criptografadas, da seguinte forma:

"*Artigo 105. os subscritos, licenciados ou as pessoas autorizadas a empregar os sistemas de radiocomunicações [...], terão as seguintes obrigações: [...] 4. Não enviar mensagens criptografadas ou em linguagem ininteligível*."

Portanto, não se deve perder de vista, para efeitos deste informe, que o contexto em que se expediu a Lei 104 de 1993 respondia a dinâmicas próprias, em que as comunicações eram vistas e funcionavam de forma muito diferente de como acontece hoje em dia. Naquela época, não existia telefonia celular (introduzida no país em 1994) nem serviço de Internet em domicílio, muito menos os serviços de mensageria instantânea e outras tecnologias semelhantes.

Por outro lado, hoje em dia, na Colômbia seguiu-se a tendência global de massificação e de popularização de serviços de telecomunicações, incluindo serviços de mensageria instantânea (tais como WhatsApp, Telegram ou Signal), que, em sua grande maioria, usam a criptografia para garantir a segurança e a privacidade nas telecomunicações.[85] Com a chegada do novo milênio, a massificação das tecnologias de telecomunicações e da Internet suporia uma revisão à limitação incluída na Lei 104 de 1993, no entanto, como se explicará adiante, tal atualização ainda é uma pendência.

84 Cujo objetivo era "*consagra[r] instrumentos para a busca da convivência, a eficácia da justiça*."

85 A esse respeito, convém consultar o resultado do projeto "El rol de los servicios OTT en el sector de las comunicaciones en Colombia 2020-2021" da Comisión de Regulación de Comunicaciones [Comissão de Regulação de comunicações] (CRC), disponível no seguinte link.

• Criptografia na Colômbia: anacronismo e ambiguidades

• Desenvolvimentos normativos

A Lei 104 de 1993, que incluiu a proibição de envio de mensagens cifradas para "*subscritos, licenciados ou as pessoas autorizadas para empregar os sistemas de radiocomunicações*"" tinha vigência original de 2 anos, não obstante, foi renovada periodicamente.[86] No entanto, nos seus trâmites legislativos, nenhuma das leis por meio das quais essa limitação ao uso da tecnologia de criptografia foi renovada chegou a ser submetida a um debate real ou a uma revisão à luz da mudança de paradigmas sociais referentes a esse uso, o que gerou uma dissociação entre a regulamentação e a realidade, que permanece até hoje.

Ao contrário, os poucos ajustes à limitação de 1993 negligenciam as problemáticas de fundo e se ocuparam, ao contrário, de ampliar a ambiguidade dessa norma. Por exemplo, o texto original da Lei 418 de 1997 estendia a proibição a pessoas autorizadas para empregar os *sistemas de radiocomunicações* entendidos como "*pagers* [...] radiotelefones portáteis, *handies* e equipamentos de radio de telefonia móvel". Por outro lado, a Lei 782 de 2002 substituiu a expressão *sistema de radiocomunicações* por "*todos os equipamentos de comunicação que utilizam espectro eletromagnético*": e esse é o texto que foi replicado na sequência. Em todo caso, o novo texto, por ser mais amplo, é ainda menos claro, uma vez que mais equipamentos usam o espectro eletromagnético de formas e contextos distintos.

Em dezembro de 2022 foi expedida a Lei 2272, por meio da qual se renovou por mais quatro anos a proibição da Lei 418 de 1997, sem que se tenha atualizado essa norma, seja eliminando a proibição ou, pelo menos, esclarecido seu alcance. Perde-se, dessa forma, mais uma vez, a oportunidade de eliminar ou, pelo menos de delimitar, uma restrição tão ambígua que, além do mais, acaba sendo anacrônica.

Somada à Lei 418 de 1997, outra Lei que se refere à criptografia é a lei de inteligência e contrainteligência colombiana (Lei 1621 de 2013). Segundo a norma, os operadores de serviços de telecomunicação devem oferecer serviços de chamadas de voz criptografadas, de forma exclusiva, a organismos que levam a cabo atividades de inteligência e contrainteligência e ao alto governo. Mesmo sendo essa norma uma obrigação direcionada a operadores de serviços de telecomunicação, considero que poderia ser interpretada como uma limitação tácita ao acesso a esse tipo de serviço oferecido pelos operadores contra a população.

• Pronunciamentos judiciais e administrativos

No âmbito do controle judicial, a Corte Constitucional revisou as disposições da Lei 104 de 1993 que originalmente introduziram a limitação ao uso de tecnologias de criptografia.

86 Primeiro, a Lei 241 de 1995 estendeu a vigência da Lei 104 de 1993 por 2 anos. Posteriormente, a Lei que a derrogou e substituiu, Ley 418 de 1997, reintroduziu a mesma proibição mencionada. A partir desse momento, a vigência da Lei 418 de 1997 foi renovada pelas leis 548 de 1999, 782 de 2002, 1106 de 2006, 1421 de 2010, 1738 de 2014, 1941 de 2018.

Todavia, a Corte[87] em 1995 considerou nesse momento que essas restrições eram compatíveis com a recém emitida Constituição Política de 1991, com relação à liberdade de expressão (Art. 20) e a privacidade (Art. 15). Segundo a Corte daquela época, considerando que o espectro eletromagnético é um bem público, os legisladores podem regulamentar o que se pode entender como seu uso correto, o que não ultrapassa as funções do legislador.

Somado a isso, a Corte argumentou que a norma acusada não era contrária à Constituição na medida em que a interceptação de comunicações deveria estar sempre antecedida por uma ordem judicial, já que a limitação da tecnologia e criptografia não implicava um acesso indiscriminado às comunicações dos cidadãos. Como veremos adiante, esse argumento em particular não resistiu à prova do tempo.

Do mesmo modo, a Corte argumentou que, se uma pessoa "não tem nada a esconder" deveria poder então sempre usar expressões usadas por *toda* a sociedade.[88] Essa análise, no entanto, não levou em conta os eventos em que uma pessoa busque exercer seu direito à vida íntima, inclusive diante do Estado, ou eventos em que, por se tratar de uma população vítima de vulnerações sistemáticas, requeiram manter altos padrões de privacidade nas comunicações, como ocorre com os membros de organizações defensoras dos direitos humanos, ambientais ou jornalistas.

De fato, existem múltiplos eventos nas últimas décadas, e sobretudo nos anos recentes, que demonstram como os argumentos da Corte de 1995 não se sustentariam diante da prova do tempo.[89] Eventos como interceptações ilegítimas de comunicações privadas por parte de entes investigativos do Estado, tal como o caso das chamadas "*chuzadas*" do Departamento Administrativo de Segurança[90] e fenômenos denunciados em publicações, tais como o Informe especial "Um estado na sombra: vigilância e ordem pública na Colômbia" emitido pela Privacy International[91] são evidências de que a vigilância do Estado não protege de maneira satisfatória os direitos à intimidade e à liberdade de expressão dos cidadãos.

No entanto, acaba sendo interessante comparar o tratamento que a Corte Constitucional dispensou à tecnologia da criptografia em 1995 com outras decisões mais recentes, como por exemplo a sentença SU-420/19,[92] decisão que se tornou um marco em matéria de liberdade de expressão emitido pela própria Corte. Nessa decisão, a Corte se referiu de forma positiva ao uso de tecnologias de criptografia por parte da população, estabelecendo que esse tipo de tecnologia tem relação estreita com a possibilidade de expressão de um indivíduo de forma anônima na internet e, portanto, são tecnologias que devem ser protegidas. Segundo a posição da Corte de 2019, o anonimato é um elemento essencial do direito à liberdade de expressão.

Segundo explicou a Corte, o anonimato responde à necessidade de neutralizar a invasão

---

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

88 O que, além de tudo, resulta em uma visão muito reducionista do uso da linguagem "comum".

89 Vale a pena mencionar que os seguintes magistrados discordaram, mediante um salvamento de voto, com os argumentos propostos no texto que foi aprovado da sentencia: Antonio Barrera Carbonell, Eduardo Cifuentes Muñoz, Carlos Gaviria Diaz Y Alejandro Martínez Ca-ballero. Por sua vez, esses Magistrados consideraram que a proibição era contrária à liberdade de expressão e à privacidade, pelo que deveria ser declarada inexequível.

90 A respeito, consultar mais detalhes do caso em:https://www.eltiempo.com/multimedia/especiales/condena-chuzadas-del-dasmaria-del-pilar-hurtado-y-bernardo-moreno/15661480/1/index.html e em https://www.semana.com/nacion/articulo/las-chuza-das/111197-3/

91 A respeito, o Informe especial pode ser consultado no seguinte link: https://privacyinternational.org/sites/default/files/2017-12/ShadowState_Espanol.pdf

92 Sentença SU-420/19. Magistrado Relator: José Fernando Reyes Cuartas.

que empresas ou governos levam a cabo na internet sobre a informação e a privacidade dos usuários. Em consequência, as tecnologias que permitem a expressão anônima dos cidadãos na internet, conforme a Corte, devem ser protegidas. Nesse sentido, cria-se ambiguidade sobre o estado atual da regulação em matéria de criptografia, uma vez que a ponderação mais recente da Corte Constitucional muda sua posição prévia sobre a matéria, mesmo quando ambas as decisões ainda estão vigentes.

Por outro lado, algumas entidades administrativas adotaram de forma tácita uma posição semelhante à versão garantista da decisão mais recente da Corte Constitucional. Mesmo que não tenham se pronunciado diretamente sobre a legalidade ou papel que a criptografia exerce na sociedade e nas telecomunicações em contraste com a Lei 418 de 1997, veem de forma favorável o emprego desse tipo de tecnologia. Alguns exemplos desses casos podem ser:

- Decisões administrativas por parte da delegação de proteção de dados pessoais da *Superintendencia de Industria y Comercio* (SIC) nas quais se questionam empresas privadas por não haver implementado adequadamente tecnologias de criptografia.[93]

- As Circulares 007 e 008 da *Superintendencia Financiera de Colombia* segundo a qual se exige de entidades vigiadas a implementação de tecnologias de criptografia para garantir proteção da informação dos consumidores financeiros.[94]

- A adoção de manuais de encriptação por parte de entidades estatais, como o *Ministerio de Educación Nacional,*[95] ou a implementação de medidas de criptografia como parte de suas políticas de segurança de informação, como o Ministério de Tecnologias de Informação e Comunicações,[96] Ministério da Saúde e Segurança Social,[97] ou a Polícia Nacional.[98]

Nesse sentido, mesmo quando não houve um pronunciamento que explicitamente modifique ou suprima as restrições incluídas na Lei 418 de 1997, tanto as autoridades administrativas como a própria Corte Constitucional promoveram o uso de tecnologias de criptografia por parte de cidadãos e entidades, inclusive ao ponto de exigi-los em alguns casos para efeitos de proteger a informação contida nas mensagens.

Não obstante, a ambivalência das posições que surge, gera insegurança jurídica e um duplo padrão, especialmente prejudicial para os cidadãos, à medida que não resulta completamente claro se o uso de tecnologias de criptografia é considerado legal. Esse fenômeno é especialmente prejudicial na Colômbia, que atualmente atravessa uma crise de vulneração de direitos e assassinatos sistemáticos de líderes ambientais e sociais,[99] os

---

93 Resolução 32129 de 2022, disponível em: https://www.sic.gov.co/sites/default/files/files/2022/22-161208%20VU.pdf

94 Disponível em: https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/10097769/f/0/c/00

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

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

97 [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

99 A esse respeito, consultar os informes realizados pela Global Witness, que localiza a Colômbia como o país com maior número de assassinatos de líderes ambientais disponível em: [https://www.globalwitness.org/es/last-line-defence-es/] y os números publicadas pelo Ins-tituto de Estudios para el Desarrollo y la Paz -INDEPAZ- em sua Radiografia da violência contra os líderes assassinados na Colômbia, disponível em [https://indepaz.org.co/wp-content/uploads/2021/09/L%C3%ADderes-ambientales-asesinados-desde-la-firma-del-acuerdo.pdf]. De igual maneira, a Defensoria Pública revelou os números alarmantes de assassinatos de líderes sociais na Colômbia, a esse respeito, se recomenda consultar: [https://www.defensoria.gov.co/-/en-los-primeros-8-meses-del-a%C3%B1o-se-han-presentado-136-homicidios-contra-l%C3%AD-deres-sociales-y-personas-defensoras-de-dd.-hh.] Estas são algumas de muitas evidências sobre a crise que atualmente atravessa o país em relação à segurança de líderes sociais e ambientais.

quais se beneficiariam da tranquilidade de contar com comunicações seguras assistidas por sistemas de encriptação.

Outro grupo especialmente afetado na Colômbia pela pouca transparência e pela falta de promoção das tecnologias de criptografia é o dos jornalistas. A esse respeito, mais especificamente pelo trabalho jornalístico realizado por meios de comunicação[100] tornaram-se públicos perfilamentos ilegítimos e perseguição a profissionais dedicados à cobertura de notícias. Nesse sentido, é claro que tecnologias de criptografia por parte de um grupo cujos direitos não são garantidos são peça-chave para evitar abusos, aumentar a segurança da informação e a privacidade desses grupos.

A respeito da incidência das decisões judiciais é importante trazer à luz que, em 2017, o então Fiscal Geral da Nação sugeriu (em um debate análogo ao que ocorreu no Brasil) que se tornasse opcional a alguns juízes colombianos ordenar que, em alguns casos de investigações criminais, se revertesse a criptografia. Apesar de a proposta não ter decolado e, portanto, não haver sido levada a um processo legislativo ou administrativo para ser implementada, é um antecedente da posição de alguns setores da sociedade que pode gerar risco para o exercício de direitos fundamentais como a privacidade ou a liberdade de expressão.[101]

• Iniciativas não governamentais

Em 2015, a Fundación Karisma já havia advertido sobre o estado ambíguo em que se encontra a regulação sobre a criptografia. No seu informe apresentado ao Relator Especial para a promoção e proteção da liberdade de opinião e expressão das Nações Unidas, David Kaye,[102] Karisma já havia denunciado a ambiguidade e o anacronismo que atualmente afetam a regulação da criptografia na colômbia, assim como os riscos associados a esas dificuldades.

Da mesma forma, a Fundación Karisma, em conjunto com a Fundación para la Libertad de Prensa (FLIP) e outras organizações não governamentais publicaram o "Manual Antiespias: *Ferramentas para a proteção digital de jornalistas*".[103] No Manual, uma das recomendações incluídas de forma reiterada é a utilização de tecnologias de criptografia nas comunicações de jornalistas de forma que se diminua o risco de afetação à privacidade e outros direitos fundamentais em caso de interceptação de comunicações.

Apesar dessas iniciativas, o tema não ganhou a atenção merecida na Colômbia assim como da parte de mais agentes não governamentais, como organizações da sociedade civil e acadêmica.

• Conclusão

Concluindo, a Colômbia permanece sem clareza a respeito de quais comunicações podem ser criptografadas, ou alcance que pode ter o monitoramento do espectro eletromagnético sem ser considerado interceptação ilegítimas de comunicações.

---

100 A esse respeito, o meio de comunicação Semana publicou a seguinte nota : [https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpetas-secretas-investigacion-semana/667616/]. De forma semelhante, El Mundo publicou a seguinte reportagem:[http://www.elmundo.com/noticia/-Perfilamientode-periodistas-compromete-al-Ejercito-colombiano/379739].

101 Disponível no link: [https://www.elespectador.com/tecnologia/romper-el-cifrado-de-whatsapp-una-mala-idea-article-687353/]

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

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

O marco ambíguo e anacrônico da regulação em matéria de encriptação na Colômbia tem efeitos negativos em duas dimensões. Por um lado, parecia impor um peso injustificada sobre a sociedade, pois restringe o uso de uma tecnologia que, tal como descreveu a Corte Constitucional na decisão SU-420/19, facilita a materialização dos direitos fundamentais de liberdade de expressão e intimidade. Em segunda medida, porque se desaproveitam as oportunidades de incentivar o uso de tecnologias de criptografia orientado a grupos em condições de vulnerabilidade, como defensores de direitos humanos, ativistas ambientais e de outras causas, assim como jornalistas.

Na Colômbia, é comum a expressão popular "quem não deve não teme" como uma desculpa para convencer alguém a divulgar informação privada. Esse é o raciocínio que levou à emissão da Lei 104 de 1993 e que sustenta a sentença C-586/95 (que vale lembrar que foi aprovada por uma maioria de 5 a 4). Não obstante, é um argumento que não é lógico no panorama atual porque a experiencia de abusos sistemáticos aos direitos dos cidadãos por parte do governo e de agentes ilegais, amplamente documentados, evidencia que se deve exigir padrões de privacidade satisfatórios, por exemplo, por meio da legitimação e promoção de tecnologias de encriptação que se mostra necessário para garantir direitos fundamentais frente aos desequilíbrios de poder existentes.

De forma semelhante ao que acontece com uma pessoa quando seu computador ou celular avisam que deve atualizar seu sistema operacional, chegou uma notificação ao Estado colombiano em letras vermelhas sobre a necessidade de revisar o estado atual das políticas públicas em matéria de criptografia.

• Recomendações

Como recomendações, para efeitos de promoção das tecnologias de criptografia para os membros da sociedade, de forma que se aproveitem os benefícios das mesmas, deve-se:

- Por parte do governo, abrir o debate sobre as mudanças que a regulação vigente requer em matéria de criptografia e seu acesso por parte dos cidadãos.

- Por parte do governo também, deve-se desenvolver políticas que promovam o uso de tecnologias de encriptação em favor de toda a sociedade e, especialmente, de grupos em risco de vulneração dos seus direitos.

- Por parte de outros setores, como a academia ou a sociedade civil, existe um chamado para promover o debate e a discussão dos efeitos da situação atual de regulação das tecnologias de criptografia para produzir soluções e recomendações pontuais.

- Por parte da sociedade, deve-se promover o uso adequado de tecnologias de criptografia como uma (de muitas) medidas necessárias para garantir materialmente direitos fundamentais como a privacidade ou a livre expressão.

- Em geral, como sociedade, a Colômbia deve realizar um chamado às autoridades, que pressione a implementar políticas públicas articuladas em matéria de criptografia e, em geral, no uso de tecnologias cujo impacto possa limitar ou beneficiar a proteção de direitos fundamentais.

Países: El Salvador, Cuba, Nicaragua e Panamá

Autores: Abdías Zambrano e Lia Hernández

Organização: IPANDETEC

Panorama geral da criptografia na América Central

• Introdução

A busca constante por soluções de segurança da informação para proteção de dados pessoais popularizou o uso da criptografia ou encriptação. Apesar disso, a região da América Central e o Caribe de língua espanhola, em geral, não regulamentaram a criptografia em nenhuma de suas normas legais, apesar do uso generalizado de aplicativos e plataformas que utilizam esse tipo de tecnologia. No entanto, El Salvador e Cuba são a exceção à regra.

Em ambos países poderemos encontrar, em geral, regulamentos de natureza distinta. Esse artigo considera os direitos que são protegidos nos dois casos por meio da encriptação, a regulamentação vigente sobre essa tecnologia analisando o estado de direito e seu uso atual pela população, considerando restrições praticadas em contraste com suas culturas de privacidade.

Também analisaremos a situação de alguns países da região considerando sua regulamentação atual em matéria de telecomunicações e privacidade de dados. O relatório também analisa a situação política atual para compreender o contexto das iniciativas legais.

• Metodologia

A metodologia utilizada para o texto aqui apresentado é completamente exploratória e qualitativa. A região não apresenta estudos ou análises aprofundadas sobre a regulamentação da criptografia que pudessem ser comparadas nessa pesquisa. Por isso, acreditamos que esta investigação pode ser uma contribuição para a comunidade acadêmica e da sociedade civil interessada nos direitos que giram em torno da criptografia.

Por se tratar de informação meramente textual, foram analisados qualitativamente os conteúdos devidamente referenciados neste relatório. Também foi utilizado um mapa comparativo global da encriptação que permite conhecer seu estado a nível internacional.

É precisamente a falta de informação o principal obstáculo encontrado para o relatório. Nos casos de Cuba e Nicarágua, a falta de digitalização dos textos legais e o rígido controle da liberdade de expressão dificultaram encontrar críticas objetivas às legislações provenientes de vozes dissidentes ou de opositores, como acadêmicos e uniões legais contrárias. Toda informação referenciada e analisada pode ser encontrada na Internet.

Por outro lado, compreender a encriptação em cada país analisado é realizar uma análise do desenvolvimento histórico legal e cultural do direito de privacidade e outros direitos desenvolvidos durante os últimos anos.

• Contexto e antecedentes

A criptografia é uma tecnologia que não deixa de ser muito discutida. Algumas pessoas creem que sua existência sem "backdoors" ou portas dos fundos permitiria o tráfico de pessoas, terrorismo, pornografia infantil e outros delitos. Porém a existência dessa porta poderia ser utilizada por outros atores, não necessariamente governamentais. A encriptação é justamente o contrário, é uma garantia de democracia e da liberdade dos cidadãos.

Entre os casos analisados, encontramos países com uma cultura política restrita à esquerda, como é o caso de Nicarágua e de Cuba. Ambos os países são acusados de manter governos ilegítimos — no caso de Cuba através de um golpe de Estado, enquanto na Nicarágua inicia-se com um processo democrático que se desvirtuou com eleições ilegítimas e sem transparência durante os últimos anos.

No caso de Cuba, uma ilha do caribe de língua espanhola, o país mantém uma ditadura com mais de cinquenta anos de funcionamento, considerada por alguns estudiosos uma democracia popular, com vernizes socialistas e comunistas. O regime cubano tem sido amplamente criticado por organismos internacionais e organizações da sociedade civil pelas constantes violações aos direitos humanos.Durante 2021 e 2022, protestos massivos contra o governo têm sido cruelmente reprimidos pelos órgãos de segurança. O país tem sido declarado pela organização internacional Freedom House, nos seus relatórios anuais mais recentes, como uma nação onde não existem liberdades online e nos espaços físicos.

Por outro lado, Nicarágua é um país que pertence ao subcontinente centroamericano. Desde 1985, de forma ininterrupta, vem sendo governada por Daniel Ortega e, desde 2017, por sua esposa como vice-presidente. Para algumas pessoas, sua forma de governo é um governo presidencialista, mas outros consideram uma ditadura por receber constantes críticas sobre seus desrespeitos aos direitos humanos, a legitimidade dos processos democráticos e a suposta violação às leis vigentes e à Constituição sobre a reeleição no país. De modo similar a Cuba, podemos observar uma constante deterioração das garantias nos espaços físicos ou digitais. Freedom House considera que a internet é parcialmente livre, enquanto é considerada sem liberdades em seu informe global de liberdades. Ao mesmo tempo que o governo vigia as comunicações dos cidadãos, opositores, religiosos, políticos, entre outros.[104]

Apesar de serem nações relativamente próximas, geograficamente falando, El Salvador e Panamá apresentam grandes diferenças quanto ao seu estado de direito e forma de governo em relação à Nicarágua e a Cuba. No caso de El Salvador, trata-se de uma república presidencialista ancorada no centro da América. Durante quarenta anos manteve governos autoritários que terminaram em guerra civil. Depois de voltar à democracia, recentemente é acusada por diversos organismos internacionais de manter um governo com verniz autoritário que não respeita a separação de poderes. Da mesma forma, é acusado de não respeitar direitos humanos e garantias fundamentais. Exemplo disso é o uso do sistema Pegasus para vigiar ativistas de direitos humanos, políticos e jornalistas de um meio de

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

comunicação de imprensa contrário ao governo.[105]

Finalmente, Panamá é uma democracia presidencialista. O país centroamericano, depois de uma ditadura, tem mantido governos eleitos democraticamente durante os últimos trinta anos e é considerado um país que assegura liberdades. Assim como El Salvador, o governo panamenho adquiriu o sistema Pegasus e posteriormente abriram-se diversas investigações e processos judiciais por espionagem e violação de privacidade das comunicações dos cidadãos.[106]

Todos os países analisados são regidos pelo direito continental e mantêm em seu ordenamento jurídico, desde suas cartas magnas até direitos e leis, normas sobre privacidade e segurança das comunicações.

• Contexto atual da encriptação na América Central

Nas sub-regiões da América Central e do Caribe não encontramos normais gerais de encriptação, porém, encontramos menções explícitas a essa tecnologia. No caso de El Salvador não existe uma lei que regule sua utilização ou, na sua falta, que a proíba, no entanto, em questões processuais e de telecomunicações, os operadores de telefonia estão obrigados a assegurar às autoridades a decodificação das comunicações de qualquer cliente, sempre e quando o serviço de encriptação tenha sido proporcionado pela companhia. Essa norma não se aplica, por exemplo, aos serviços de mensagens móveis globais mais populares, ainda que seus usuários vivam em território salvadorenho, a não ser que seja um serviço operado e oferecido por companhias que operam neste país. Essa lei oferece uma descrição clara do que é encriptação: sistema através do qual, com ajuda de técnicas diversas ou programas informáticos, determinada informação é cifrada ou codificada com a finalidade de torná-la inacessível ou inteligível a quem não está autorizado a ter acesso a ela.

Outra norma que menciona a encriptação no ordenamento jurídico salvadorenho é a Lei especial de Telecomunicações. Na seção sobre material não decodificado, é mencionado o procedimento que as entidades investigativas devem seguir caso não consigam decodificar um material criptografado. Ambas as leis apresentam certos princípios que buscam salvaguardar direitos humanos, compromissos internacionais e garantias dos cidadãos, como o direito à privacidade e intimidade, especificamente a privacidade, a temporalidade, a reserva e a confidencialidade.

Cabe mencionar que El Salvador é um dos países da América Central onde a proteção de dados pessoais não está desenvolvida por meio de um texto único, deixando de considerar regras novas para a custódia e a transferência dos mesmos. Durante a pandemia, foi discutido um projeto de lei visando garantir que o titular dos dados e os interessados pudessem encontrar um equilíbrio entre o respeito aos direitos online sem parar o desenvolvimento da Internet, o uso efetivo das telecomunicações e o avanço das tecnologias de informação e comunicação, porém, não foi sancionado pelo novo governo com o compromisso de apresentar e aprovar em breve uma lei de dados pessoais.

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

No caso de Cuba, a criptografia e sua regulamentação tem sido mais polêmica. Em 2008 se aprovou uma resolução que contemplava uma proibição expressa da criptografia por parte do Ministério da Informática e das Comunicações.[107] No entanto, reformas de 2011 e 2017 permitiram o uso da encriptação de dados através de uma permissão que o provedor de internet recebe.[108] Em razão dessa regulamentação excessiva e violatória da privacidade das comunicações, o relator especial para a liberdade de opinião e expressão da Organização das Nações Unidas criticou em 2015, através de um relatório, tal resolução. Em seu relatório, o autor expressa que a regulamentação da criptografia não permite um livre exercício da opinião, além de deixar que o governo possa intervir nas comunicações de seus cidadãos.[109]

Apesar dessa proibição, plataformas de mensagens instantâneas como WhatsApp e Telegram são amplamente utilizadas na ilha. Em 2020, o Telegram foi bloqueado por cinco semanas[110]. A situação se repetiu em 2021, em meio dos maiores protestos desde 1959, o governo bloqueou muitos aplicativos criptografados nas redes 3G e 4G, além de deixar a ilha sem internet.[111] Nesse mesmo ano, o governo apresentou um decreto-lei que menciona multas a quem utilizar encriptação sem a devida inscrição.[112] Essa nova lei incendiou novamente os debates internacionais e as críticas de governos e organizações da sociedade civil pela violações aos direitos humanos.[113]

Ativistas dos direitos humanos têm denunciado as más condutas de empresas que revelam dados pessoais[114]. Durante 2022 foi aprovada uma lei de dados pessoais que entrará em vigor em 2023, sendo criticada por sua ambiguidade a respeito das exceções de tratamento sobre consentimento do titular, especificamente "por razões de segurança coletiva, bem-estar geral, respeito à ordem pública e interesse de defesa"[115].

No caso de Nicarágua e Panamá, encontramos que em nenhum dos países se menciona uma regulamentação nacional da criptografia. Ambos os países mantêm a nível constitucional a privacidade das comunicações e leis de dados pessoais. No caso da Nicarágua, sua lei de dados pessoais não é aplicada e o órgão responsável não está em operação.

Considerando a norma legal, pode-se interceptar as comunicações de qualquer natureza desde que reúnam determinadas características relacionadas com o crime investigado caso em posse de uma ordem judicial[116]. Apesar disso, a interceptação das comunicações pode ser feita mesmo sem a ordem se nas 24 horas seguintes for recebida uma solicitação de um juíz[117]. Nesse mesmo sentido, uma iniciativa de 2015 propunha obrigar as empresas

---

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-internet-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_c07y586

112 Decreto Ley 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=nhKojgRp5_A Emil,

115 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-

provedoras de internet a dar acesso a qualquer informação que o governo nicaraguense desejasse[118]. A iniciativa foi descartada depois de críticas de opositores e da sociedade civil.

Durante a pandemia, um informe de LACNIC determinou a urgência de minimizar a ingerência das autoridades no país[119]. Durante os protestos de 2018 foram reportadas situações em que a Polícia obrigava manifestantes a desbloquear seus celulares para ler suas conversas, não importando a criptografia[120]. Jornalistas e defensores dos direitos humanos relataram a importância da encriptação para seus trabalhos e ativismo apesar das limitações que as plataformas apresentam à atividade jornalística.[121]

No caso do Panamá, existe uma lei de proteção de dados pessoais que recentemente foi promulgada e entrou em vigor. Da mesma forma, sua norma penal permite a interceptação de comunicações desde que motivada por uma resolução judicial.[122] Diferente dos demais países analisados, o assédio jornalístico mais comum é de tipo judicial até o momento.[123]

Além disso, a criptografia foi utilizada durante a pandemia pelas autoridades para elaborar respostas à pandemia de Covid-19.[124] Por outro lado, em 2021 foi reportado um vazamento de um projeto de decisão judicial encriptado que pertencia a um dos magistrados da Suprema Corte de Justiça.[125] O projeto tratava de uma ação de inconstitucionalidade relativa a um ex-presidente do país que fora acusado de violar as comunicações. A situação foi uma das poucas em nível nacional em que se menciona a criptografia.

Por outro lado, a encriptação é mencionada como garantia da prática da sexualidade de minorias sexuais pela Internet Society.[126] A equipe médica usa criptografia para se comunicar com pacientes transgêneros, para que eles se sintam confiantes de que suas informações não serão vazadas. Da mesma forma, protege as pessoas LGBTQIA+ de sofrer discriminação ao escolher compartilhar sua orientação ou identidade de gênero e ajuda adolescentes e jovens que vivem em países onde suas orientações sexuais são proibidas a se comunicar com seus pares em outros países.

Nos casos dos países estudados, ser um pessoa LGBTQIA+ não é proibido, no entanto, existe uma ampla discriminação. Cuba é o único que permite o matrimônio igualitário, portanto, é conclusivo dizer que pessoas LGBTQIA+ de Cuba, Nicarágua, Panamá e El Salvador usam serviços de mensagens criptografadas para sua segurança. Isso demonstra

-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://ondalocalni.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? (2022). Despacho 505. https://www.despacho505.com/presuma-que-toda-comuni-cacion-esta-intervenida-como-enfrentar-el-espionaje-del-regimen-ortega-murillo/ ; Redacción Confidencial. (2022). La guerra de Daniel Ortega contra el periodismo: 54 medios cerrados. Confidencial. https://www.confidencial.digital/politica/54-medios-cerrados-guerra-daniel-ortega--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

124 Sanchez, A. C. (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/filtracion-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/

que, além dos direitos mencionados, assegura os direitos de autodeterminação e identidade.

• Conclusão

Depois da análise anterior não restam dúvidas de que a encriptação assegura direitos humanos vitais e reforça a necessidade de que governos e sociedades façam tudo o que for possível para assegurar seu funcionamento.

Nos casos estudados pudemos ver como a situação da criptografia muda segundo o regime político do país. Os direitos de privacidade, liberdade de expressão, associação e dados pessoais se encontram consagrados de forma direta ou indireta em todas as Constituições do continente, portanto os direitos humanos se mesclam com os direitos políticos no caso do uso de novas tecnologias.

Desde ditaduras como a cubana onde se controla a criptografia, passando por um regime autoritário sem recursos para dar seguimento à encriptação como a Nicarágua, examinamos também a democracia em transformação de El Salvador, para finalmente analisar uma democracia de liberdades plenas como Panamá onde não se regula a criptografia.

Ao mesmo tempo, pode-se entender que, nos países onde não existe nenhuma menção à criptografia na regulamentação, existe seu uso generalizado. É o caso do Panamá, onde existe um apoio tácito ao seu uso em nível governamental.

Por outro lado, a liberdade de imprensa se vê salvaguardada graças à encriptação. Jornalistas recorrem a essa tecnologia para proteger suas fontes de investigação de pessoas opositoras ou atores governamentais, sobretudo em governos autoritários como o da Nicarágua. De maneira semelhante, pudemos ver outros direitos salvaguardados como o direito à autodeterminação e identidade de pessoas LGBTQIA+.

• Recomendações

- É necessário que os governos analisados respeitem a privacidade das comunicações através do respeito das leis de garantia vigentes e a formulação de políticas públicas que busquem essa garantia.
- Por outro lado, alguns dos países analisados, como Cuba e El Salvador, devem reformular suas leis atuais ou revogá-las dando espaço a novos textos legais compatíveis com os direitos humanos.
- Da mesma forma, é necessária a discussão ou atualização das leis que protegem os dados pessoais na região.
- Por último, os governos devem fazer tudo o que for possível para difundir a encriptação para minorías étnicas e raciais, defensores dos direitos humanos e jornalistas. Fazer isso supõe um compromisso com a democracia.

País: Venezuela

Autor: Rómulo Chacín González

A criptografia na Venezuela: impacto das políticas nos direitos fundamentais

• Introdução

Existe, em nível mundial, uma tendência cada vez mais frequente por parte dos governos e dos cibercriminosos a ter acesso a informações de terceiros por múltiplas razões. No entanto, o caso da Venezuela é especialmente alarmante na região dado que a violação dos direitos fundamentais é uma prática institucionalizada e sistemática, dando lugar ao cometimento de crimes contra a humanidade.

A configuração do cenário é propícia para eles pois, além de tudo, não existem instituições imparciais e efetivas que protejam o indivíduo frente a tais atropelos, assim como não existe uma legislação robusta na questão de proteger dados pessoais. Em contraste com isso, existe uma grande quantidade de agências de inteligência criadas por Decretos do Poder Executivo que operam à discrição do regime cujas faculdades são ambíguas e permitem ser acomodadas em prejuízo dos indivíduos, em clara contradição com os princípios de legalidade, necessidade, proporcionalidade e o processo devido.

Diante de tal cenário, o uso de criptografia se apresenta como um direito que conta com cobertura constitucional e como uma necessidade das pessoas para evadirem da incessante vigilância estatal, assim como da cibercriminalidade; pois isso tende a garantir a privacidade das comunicações e da informação em geral.

Por tudo isso, propomos com este relatório realizar um estudo das ações mais relevantes implantadas na Venezuela, tanto a favor da criptografia como contra ela, a fim de determinar seu impacto nos direitos dos indivíduos, fundamentalmente quanto à liberdade de expressão, privacidade, proteção de dados pessoais e segurança.

• Metodologia

A investigação realizada foi de tipo documental com revisão crítica do estado do conhecimento, em nível exploratório. O processo se baseou na busca, coleta, análise, crítica e interpretação de dados e de informações contidas nas fontes documentais impressas e eletrônicas, fundamentalmente em relatórios de instituições privadas venezuelanas e organizações de Direitos Humanos, assim como de normas jurídicas relacionadas direta ou indiretamente com a criptografia. Com isso se pretende elaborar esse tema na Venezuela contribuindo com os poucos estudos existentes.

• Contexto e antecedentes

A Venezuela atravessa desde 2014 uma das mais profundas e complexas crises em nível global, especialmente no que diz respeito à situação dos Direitos Humanos. Torturas, desaparições forçadas, execuções extrajudiciais, prisões arbitrárias,[127] apreensões ilegais e interceptação de comunicações são algumas ferramentas de uso cotidiano por parte das autoridades e de seus colaboradores. O direito à privacidade tem sido um dos mais afetados através da vigilância que as agências de inteligências do Estado, CONATAL e CANTV, exercem sobre as comunicações por razões políticas.[128] De fato, é comum escutar conversas privadas gravadas no canal de televisão do governo para deixar em evidência os afetados, o que demonstra a gravidade da situação.

Com relação a isso, o setor privado[129] também tem participado destas condutas de vigilância a pedido das agências do regime. Em 2021, a Telefónica interceptou linhas na Venezuela,[130] número que apresenta um nítido e constante aumento desde 2016. Como bem aponta Vesinfiltro,[131] isso equivale a mais de 20% de seus assinantes no país, sendo que no resto das nações nas quais a empresa opera esse número não alcança nem 1%.

Outra poderosa ferramenta do Estado para intervir sobre as liberdades individuais é a censura. A esse respeito, a Espacio Público estima que entre os anos de 2003 e 2022 foram fechadas ao menos 215 emissoras de rádio em todo território nacional. De fato, a censura alcançou 39% das violações à liberdade de expressão em 2022.[132]

Esses fatos se somam a outros igualmente graves como o bloqueio de TOR e de outras ferramentas para a evasão à censura, como redes privadas virtuais e protocolos de comunicação *Hypertext Transfer Protocol Secure* (HTTPS)[133] em alguns websites[134] que funcionam como meios de comunicação e de informação. Cabe destacar que todas essas tecnologias fazem um importante uso da criptografia.

Não à toa, a Venezuela foi catalogada como um dos países com menor liberdade de internet no mundo com uma avaliação de 30/100 pontos,[135] qualificação que a deixa em penúltimo lugar em comparação aos demais países latino-americanos.

---

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

128 Privacy International. (2016). The Right to Privacy in Venezuela. Disponível em: https://www.privacyinternational.org/sites/default/files/2017-12/venezuela_upr2016.pdf .

129 Departamento de Estado. (2020). Country Reports on Human Rights Practices: Venezuela. Disponível em: 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. Disponível em: 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. Disponível em: 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

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

• Políticas relacionadas à criptografia

A inviolabilidade das comunicações privadas se encontra consagrada pela Constituição da República Bolivariana da Venezuela[136] (CRBV) em seu Art. 48, o qual garante o segredo e a inviolabilidade em todas suas formas. Assim, as coisas, tanto pessoais naturais como pessoas jurídicas gozam do direito à confidencialidade de seus conteúdos, de forma tal que a informação seja inacessível a terceiros não desejados, implicando como consequência que somente aqueles autorizados podem acessá-la.

Em relação a isso, convém destacar que todas as pessoas são titulares deste direito sem importar o meio de comunicação, podendo ser escrito, virtual, sonoro, entre outros; e que tais comunicações somente poderão ser interceptadas mediante ordem judicial correspondente. Por outro lado, o Art. 60 *ejusdem* reconhece os direitos à proteção da "honra, vida privada, intimidade, autoimagem, confidencialidade e reputação". Do conteúdo dessas duas normas de ordem constitucional deriva o poder dos indivíduos presentes no território da República de proteger suas comunicações e, em geral, qualquer tipo de informação através dos meios que avaliem apropriados para tal finalidade. Como conclusão óbvia, a criptografia é um desses meios.

No parágrafo 2 do Art. 12 da Lei Orgânica de Telecomunicações[137] se reconhece o direito dos usuários à privacidade e à inviolabilidade de suas telecomunicações, excetuando-se aqueles casos expressamente autorizados pela CRBV ou que sejam de interesse público.

Seu regulamento para a proteção dos direitos dos usuários nas prestações de serviços de Telecomunicações (2018)[138] estabelece no seu Art. 7 o dever dos operadores de prever mecanismos para resguardar o segredo e a inviolabilidade das comunicações privadas que circulam em suas redes. Deste mesmo modo, seu Art. 30 assinala que esses deveram adotar mecanismos que garantam a confidencialidade dos dados pessoais.

O parágrafo 2 do Art. 18 da Lei Orgânica de Reforma Parcial do Decreto com Grau, Valor e Vigência da Lei Orgânica de Ciência, Tecnologia e Inovação[139] estabelece que a autoridade nacional competente nesta matéria deverá resguardar a inviolabilidade e o caráter confidencial dos dados eletrônicos obtidos no exercício das funções dos órgãos e entes públicos. Também, no parágrafo 22 do Art. 19 dispõe entre as competências do órgão de controle o estabelecimento de políticas, normas e medidas técnicas orientadas a resguardar a privacidade, confidencialidade e inviolabilidade das pessoas.

Em relação a isso, o Centro Nacional de Tecnologias da Informação publicou em 2011 o Marco de Interoperabilidade (MIO) para integrar os serviços do Estado, outorgando uma grande importância à criptografia como componente da camada de segurança na troca eletrônica de dados entre suas instituições.[140] A Superintendência de Serviços de Certificação Eletrônica (SUSCERTE) também faz bastante uso da criptografia como método para proteger

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 na Gaceta Oficial Nro. 39.610 del 7 de febrero de 2011. Disponível em: https://www.asambleanacional.gob.ve/storage/documentos/leyes/ley-de-ref-20220117162719.pdf.

138 Disponível em: 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. Disponível em: https://www.asambleanacional.gob.ve/storage/documentos/leyes/ley-de-ref-20220609123842.pdf.

140 Disponível em: https://www.cnti.gob.ve/phocadownload/publicaciones/mio.pdf.

cópias de segurança de suas chaves privadas e exportá-las para outros componentes do sistema.[141]

Por sua vez, os Arts. 23 e 25 da Lei de Infogoverno[142] estabelecem tanto o princípio de segurança como o de proteção de dados pessoais, em relação ao uso de tecnologias de informação por parte do Poder Público e do Poder Popular. A respeito disso, deve-se garantir a integridade, confidencialidade, autenticidade e disponibilidade da informação, documentos e comunicações eletrônicas. Além disso, o segundo estabelece o dever de respeitar a honra, vida privada, intimidade, a autoimagem, confidencialidade e a reputação das pessoas. Por outro lado, no Art. 55.4 aponta a SUSCERTE a articulação e a inserção de iniciativas em matéria de segurança informática.

O artigo 173 do Decreto com Grau, Vigência e Força de Lei das Instituições do Setor Bancário[143] estabelece as atribuições e funções em matéria de segurança bancária da Superintendência das Instituições do Setor Bancário. Dentre elas, destaca-se a de número 1 para garantir que tais instituições tenham os sistemas e procedimentos necessários para minimizar a presença de fraudes em suas operações. A partir disso, no Art. 20 da Resolução Nº 641-10[144] da Superintendencia citada, de data 23 de dezembro de 2010, ficou estabelecido que esses devem implementar uma criptografia robusta para proteger o canal de comunicação. No mesmo sentido, a disposição expressa no Art. 21 que prevê às instituições o dever de implementar mecanismos criptografados de transmissão e armazenamento da informação, a fim de evitar que os dados sensíveis sejam conhecidos por terceiros não autorizados. Isso foi reafirmado na alínea "m" do Art. 23 da Resolução Nº 001.21, de 04 de janeiro de 2021.

Outros textos normativos que abordam o tema da confidencialidade, integridade, privacidade e, em geral, da segurança das comunicações e dos dados e informações são o Decreto com Força de Lei sobre Mensagens de dados e Firmas eletrônicas,[145] o Decreto com Grau, Valor e Força de Lei sobre o Acesso e Intercâmbio Eletrônico de Dados, Informações e Documentos entre os Órgãos e Entidades do Estado,[146] bem como a Lei de Proteção da Privacidade das Comunicações.[147]

Dizendo de outro modo, cabe destacar que a Venezuela não conta com uma legislação integral sobre a questão da proteção de dados pessoais, a Sala Constitucional de nosso mais alto tribunal estabeleceu importantes diretrizes que devem ser observadas em relação à "... toda normativa ou sistema sobre dados pessoais que contenham informações de qualquer tipo referida a pessoas físicas ou jurídicas determinadas ou determináveis...". Entre os aspectos mais relevantes, destaca-se o princípio da segurança e confidencialidade, de acordo com o qual "deverão ser adotadas medidas técnicas e organizativas que forem necessárias para proteger os dados contra alteração, perda ou destruição acidental e acesso não

---

141 Disponível em: http://www.suscerte.gob.ve/dpc/DPC.pdf.

142 Publicada na Gaceta Oficial Nro. 40.274 del 17 de octubre de 2013. Disponível em: 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. Disponível em: 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. Disponível em: https://www.asambleanacional.gob.ve/storage/documentos/leyes/decreto-no-20220315144506.pdf

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.

autorizado ou uso fraudulento".

O aplicativo WhatsApp é, talvez, a ferramenta de comunicação mais usada na Venezuela no que se refere a mensagens pessoais e chamadas. Seu uso é tão importante no país que é considerado um canal de informação para a maioria da população[148] em virtude da desinformação que impera. Esse aplicativo emprega um mecanismo de criptografia assimétrico de ponta a ponta desde 2016, o que implica em ninguém ter acesso ao conteúdo das comunicações (vídeos, áudio, imagens, arquivos, chamadas, videochamadas ou mensagens) em formato legível, garantindo assim a confidencialidade como atributo da segurança da informação.[149] Outros aplicativos similares amplamente utilizados são o Telegram e o Signal.

Os privados também se beneficiam da criptografia para realizar pagamentos em nuvem[150] e transações bancárias,[151] assim como para navegar pela internet graças ao protocolo HTTPS — promovido por organizações como WordPress Venezuela[152] e, em geral, a criptografia é patrocinada por ONGs como ISOC Venezuela e Vesinfiltro.

Em clara contradição com o que foi apresentado anteriormente, destacamos a grande quantidade de agências de inteligência do Estado e a indeterminação de suas faculdades em direitos que restringem as liberdades; o marco normativo digital ambíguo e disperso, a precariedade de regulamentações relativas a proteção de dados pessoas e a ausência absoluta de mecanismos de controle efetivos e imparciais. Isso configura, sem dúvida, um ambiente propício de vigilância em que se torna fácil suprimir a liberdade de expressão, prejudicando gravemente o ambiente necessário para uma sociedade democrática.[153]

Existem evidências razoáveis para crer que a empresa israelense Cellebrite vendeu tecnologia de pirataria telefônica para o regime de Maduro sob supostas alegações de combate à criminalidade. Cabe destacar que a ferramenta em questão pode desbloquear e extrair dados de telefones móveis incluindo os dados encriptados,[154] o que gera grande preocupação devido ao nível exagerado de desprezo dos Direitos Humanos na Venezuela.

Embora não se evidencie uma conduta generalizada e sistemática contra a criptografia, é necessário destacar que várias redes privadas virtuais (VPN) e alguns provedores privados[155] foram bloqueadas pela CANTV, uma vez que têm sido utilizados pela população como forma de driblar a censura em diversos meios e a vigilância estatal. Exemplos de algumas dessas redes bloqueadas são TunnelBear e Psiphon.[156]

---

148 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.

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

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

151 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."

152 Disponível em: https://ve.wordpress.org/support/article/why-should-i-use-https/

153 Derechos Digitales. (2018). Políticas Públicas para el Acceso a Internet en Venezuela. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/CPI_venezuela.pdf

154 Freedom House. (2022). Libertad en la Red: Venezuela. Disponível em: https://freedomhouse.org/country/venezuela/freedom-net/2022

155 Vesinfltro (2021) Report: Digital rights, censorship, and connectivity in Venezuela. Disponível em: https://vesinfiltro.com/noticias/2021_annual_report

156 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 .

Além disso, também existem evidências de que a Venezuela iniciou negociações que levaram à aquisição do *Remote Control System* (RCS) do *Hacking Team* no ano de 2013, ferramenta que permite acesso a correspondências e comunicações criptografadas.[157] Entre os mais afetados por essas práticas abusivas do Estado venezuelano estão ativistas,[158] defensores de direitos humanos, políticos e qualquer pessoa que tenha alguma vinculação política contrária ao regime. No entanto, como pôde ser visto no referido relatório da Telefónica, todos são realmente um alvo potencial para essas ações.

• Conclusão

A proteção das comunicações e, em geral, qualquer tipo de informação é um direito que conta com cobertura constitucional na Venezuela, assim como com um desenvolvido regulamento no âmbito legal e sublegal. Tal proteção pode ser realizada através de ferramentas como a criptografia. Embora sejam poucas as normas que aludem à criptografia de forma direta, isso não nos impede de considerar que seu uso, como o de outras ferramentas e técnicas de segurança, é um direito que decorre da inviolabilidade das comunicações privadas e do direito à proteção pessoal.

Não existe um marco jurídico sólido no que diz respeito à proteção de dados pessoais, o que nos distancia dos padrões internacionais sobre a matéria e deixa as pessoas em situação de vulnerabilidade na ausência de mecanismos e instituições especializadas, imparciais e eficazes.

Os ataques às liberdades são comuns em nossa região, no entanto, o caso da Venezuela é especialmente alarmante e a situação favorece práticas abusivas por parte do Estado. A inumerável quantidade de agências de inteligência do regime, um Poder Judicial ineficiente a serviço dele e a politização generalizada do acesso aos bens e serviços são alguns dos elementos essenciais para tal situação.
Não se evidencia uma conduta generalizada e sistemática que aponte especialmente contra a criptografia na Venezuela; no entanto, isso pode ser esperado da censura e vigilância como políticas institucionalizadas. Algumas dessas políticas conseguiram impactar negativamente a criptografia.

Tudo isso, aliado à desconfiança geral da população em relação às instituições públicas e seus representantes, fazem da criptografia uma ferramenta poderosa e necessária para a proteção das informações e comunicações, para lidar não apenas com práticas abusivas do Estado, mas também para as atividades maliciosas dos cibercriminosos.

• Recomendações

- Sugere-se a todos os órgãos e entes do Poder Público em todos os níveis que protejam e promovam o uso de criptografia forte de ponta a ponta através de políticas correspondentes, pois isso tende a garantir a segurança de milhões de pessoas, assim como a segurança do país. Assim, devem ser abandonadas quaisquer práticas que lesem direta ou indiretamente a criptografia.

157 Derechos Digitales. (2016). Informe: Hacking Team Malware para la Vigilancia en América Latina. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf. p.9.

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

• Recomenda-se a todas as pessoas a adoção de criptografia forte no que diz respeito a suas informações e comunicações, pois é a ferramenta mais consistente disponível para proteção dessas. Recomendamos em especial a adoção para ativistas, defensores dos direitos humanos, jornalistas e para todos vinculados de forma direta ou indireta com atividades políticas.

• Urge o Poder Legislativo discutir e aprovar uma lei de proteção de dados pessoais que elabore normas constitucionais sobre a questão e que sigam os padrões internacionais de proteção. Também é importante realizar uma revisão exaustiva das normas e práticas que restringem a liberdade de expressão e o direito de comunicar-se livremente e, em todo caso, modificá-las para que acatem os princípios de legalidade, necessidade, proporcionalidade e o devido processo legal.