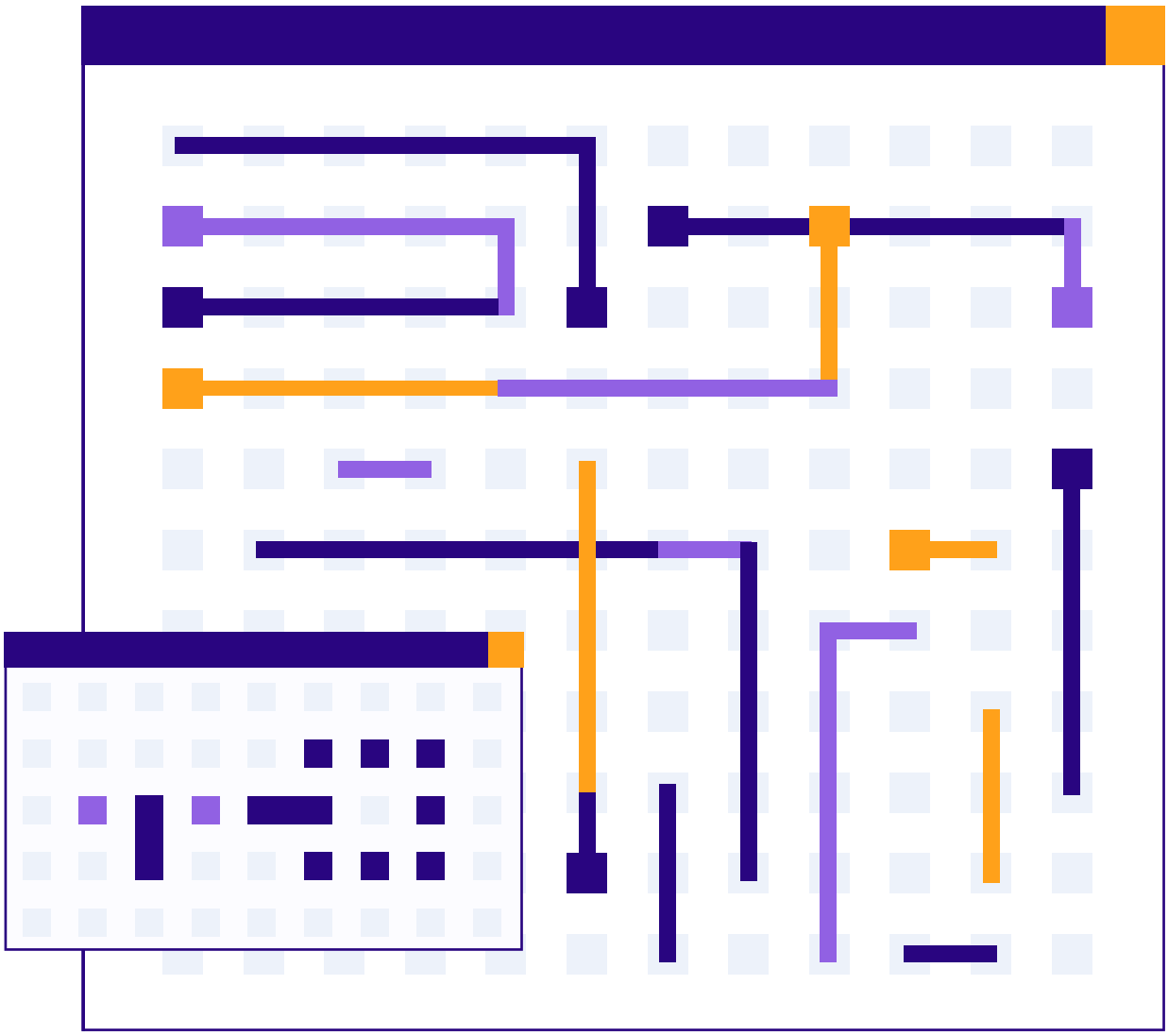
PERCEPCIONES SOBRE EL CIFRADO Y INVESTIGACIONES CRIMINALES

mapeo y análisis



INSTITUTO DE REFERENCIA EN INTERNET Y SOCIEDAD

apoyo:

Internet Society Capítulo Brasil

Internet Society Foundation

PERCEPCIONES SOBRE EL CIFRADO Y INVESTIGACIONES CRIMINALES

mapeo y análisis

Autores

Ana Bárbara Gomes Pereira

Gustavo Ramos Rodrigues

Victor Barbieri Rodrigues Vieira

Consultoría

Lucas Caetano Pereira de Oliveira

Revisión externa

Paulo Rená da Silva Santarém

Raquel Lima Saraiva

Traducción

Zenaide Silva

Portada, diseño gráfico y maquetación

Felipe Duarte

Esta publicación es parte del proyecto "**Privacidad es seguridad: Comunicar la importancia del cifrado para todos**", en alianza con ISOC Brasil y con financiamiento de ISOC Foundation.

logro: IRIS INSTITUTO DE REFERENCIA EN INTERNET Y SOCIEDAD

apoyo: Internet Society Capítulo Brasil · Internet Society Foundation

INSTITUTO
DE REFERENCIA
EN INTERNET
Y SOCIEDAD

DIRECCIÓN

Luíza Couto Chaves Brandão

MIEMBROS

Ana Bárbara Gomes / Investigadora

Beatriz Fernandes / Pasante de Comunicación

Felipe Duarte / Coordinador de Comunicación

Gustavo Rodrigues / Coordinador de Políticas Públicas e Investigador

Juliana Roman / Investigadora

Lahis Kurtz / Coordinadora de Investigación e Investigadora

Leandro Soares Nunes / Investigador

Paloma Rocillo Rolim do Carmo / Vice-directora e Investigadora

Pedro Vilela Resende Gonçalves / Co-fundador y asociado

Victor Barbieri Rodrigues Vieira / Investigador

RESÚMEN

Resúmen ejecutivo

Contexto. Desde la segunda mitad del siglo XX, el constante avance tecnológico en el campo de las técnicas cifradas, como también las perspectivas de masificación del acceso a esas tecnologías por parte de la sociedad civil ha representado un punto de recurrente conflicto argumentativo. Demarcada por lo que se ha convenido llamar *Crypto Wars* – o Guerras Criptográficas – la disputa que involucra Estado, industria y sociedad civil alrededor del derecho de acceso de esta a técnicas de cifrado fuerte y segura se amplía hasta los días actuales. De naturaleza episódica – pero perene – las Guerras Criptográficas adquieren nuevas dimensiones en el siglo XXI, con el exponencial aumento del acceso de la sociedad civil a la internet y, concomitantemente, con el desarrollo y uso de tecnologías investigativas cada vez más sofisticadas.

En Brasil, la importación de la narrativa estadounidense del *Going Dark* – o "oscurecimiento" – culminó también en la reproducción de ese conflicto, materializado inicialmente en los bloqueos de la aplicación WhatsApp en el país en 2015 y 2016. Los casos culminaron en la ADI 5527 y ADPF 403, impetradas en el Supremo Tribunal Federal, que tematizan la constitucionalidad de las medidas. Aunque la conclusión del juicio de ambas estar todavía pendiente, los votos de los relatores de esas acciones indicaron el reconocimiento del cifrado como esencial a la realización de derechos fundamentales, como privacidad y libertad de expresión. Similarmente, el Superior Tribunal de Justicia ya ha considerado, en los exámenes del RMS 60.531 y del RESP 1.872.695, ilícita la aplicación de sanciones a proveedor de aplicación que incumple orden de interceptación por imposibilidad técnica imposta por el cifrado.

A pesar de eso, intentos de introducir un mecanismo de acceso excepcional en la cifrado todavía ocurren en el país y no raramente se tornan objeto de discusión legislativa. El apodado "Paquete Anti Crimen" del ex-Ministro de la Justicia y Seguridad Pública Sérgio Moro, contenía previsiones que ampliaron los poderes de interceptación estatales y podrían implicar en una fragilización del cifrado, por ejemplo. Similarmente, la reforma del Código de Proceso Penal ha sacado a la luz el debate sobre la posibilidad de proveedores de aplicación ser compelidos a la reducción de la seguridad de sus sistemas para realización de interceptaciones durante la persecución penal. De ese modo, la cuestión del acceso excepcional y de la gobernanza de cifrado sigue urgente y actual en el país.

Metodología. En ese contexto, el presente estudio buscó investigar las percepciones y opiniones de profesionales involucrados con el debate público sobre el tema. Se realizaron 45 entrevistas, de las cuales 43 se consideraron válidas, con representantes de los sectores gubernamentales , empresarial, tercer sector y comunidad científica y tecnológica. Los profesionales presentaron diferentes formaciones disciplinares y trayectorias profesionales.

Se seleccionaron los entrevistados por medio del método de muestreo en “pelota de nieve,” en el que los participantes son indicados por los anteriores, creando una red social progresivamente expandida. Una vez que ese método no genera un muestreo representativo de ningún segmento poblacional y es más sensible a perspectivas de selección, no se debe entender el presente estudio como una pesquisa de opinión, sino como un mapeo empírico y análisis de los principales discursos, racionalidades y creencias que permean las guerras criptográficas brasileñas.

Después de las entrevistas, se realizó la codificación y análisis de las percepciones y opiniones de esos profesionales en relación a cuatro tópicos: i) implementación de acceso excepcional en sistemas cifrados para acceso a datos cifrados para fines de persecución penal; ii) conocimientos y riesgos sobre potenciales alternativas para acceso de las autoridades al contenido cifrado sin interferencia directa en el cifrado; iii) el ambiente regulatorio nacional referente al cifrado; y iv) los bloqueos de WhatsApp en Brasil y su relación con el Marco Civil de Internet. Se presentaron los resultados de ese análisis bajo forma de reconstrucciones narrativas de los discursos identificados. Hecho ese mapeo , se procedió a un análisis de las relaciones entre las tesis identificadas y los contextos factuales con los que se relacionan.

Resultados. En relación al acceso excepcional, se constataron dos discursos principales en torno del tema. El discurso favorable a la medida entiende existir hoy un conflicto esencial entre privacidad y seguridad pública y supone la primacía de ese último valor sobre el primero. Entiende, todavía, existir en el derecho brasileño un deber legal de garantizar las condiciones para que las interceptaciones ocurran por parte de aquellos que se pueden compelir a su realización en los términos de la ley. Paralelamente, el discurso contrario al acceso excepcional considera la medida desproporcionalmente dañosa, pues esta atingiría a todos los usuarios del sistema, comprometiendo su seguridad informacional y sus derechos fundamentales, además de perjudicar la confianza en el ambiente digital. Además, cuestiona tanto la necesidad efectiva de la medida cuanto su eficacia alegada, sugiriendo que la criminalidad migrará de las plataformas comprometidas.

Cuanto a posibles alternativas para el acceso a datos sin violación delcifrado, las principales alternativas citadas fueron la aprensión y desbloqueo de los dispositivos de las personas investigadas, hacking gubernamental de esos dispositivos, análisis de metadatos, *client side-scanning*, inserción de un usuario fantasma y el acceso a datos almacenados en servicios de nube. Con relación a las soluciones basadas en el comprometimiento de la seguridad del dispositivo individual, se apuntó un riesgo de violación de los derechos del investigado, teniendo en cuenta la posibilidad de acceso a cualquiera contenido del dispositivo, incluso aquellos irrelevantes para la investigación. Cuanto a las soluciones de *client-side scanning* e inserción de un usuario fantasma, la suposición de que tales soluciones no interferirían en el cifrado fue objeto de cuestionamiento y crítica. En ese sentido, una percepción frecuente fue la de que habría un comprometimiento “principiológico” del cifrado aunque sin una interferencia directa en el algoritmo criptográfico o en el sistema de gestión de llaves.

Cuanto al ambiente regulatorio relativo al cifrado en Brasil, una percepción frecuente fue la de ambivalencia: el cifrado sería simultáneamente valorizad y amenazado. La valorización provendría de normas como la Ley General de Protección de Datos, el Marco Civil de Internet y el Decreto nº 8771/2016, las cuales se perciben como incentivos al uso de ese recurso por la sociedad, aunque en la ausencia de referencia expresa en el caso de las dos leyes. Similarmente, los votos de los relatores de las acciones sobre el tema en el STF y la jurisprudencia del STJ fueron citados como indicadores de un reconocimiento de la importancia del cifrado en la institucionalidad brasileña. Por otro lado, el carácter inconcluso del juicio de las acciones en el STF y las tentativas recurrentes de introducir acceso excepcional fueron vistas como señales de que el cifrado sigue amenazado en el país.

En ese punto, dos discursos distintos sobre la cuestión de la regulación del cifrado emergieron . Uno de ellos defiende la introducción de garantías explícitas en la legislación , sea por medio de una afirmación legal expresada de que el empleo de cifrado por ciudadanos y empresas es lícito, sea por la conversión de los incentivos actuales al empleo de cifrado en un deber vinculativo aplicable a ciertos proveedores y aplicaciones. Por otro lado, el segundo discurso cuestiona si la referencia legal expresada a el cifrado sería positioa, entendiendo que tal enfoque es ideal de neutralidad tecnológica de la regulación y puede representar una interferencia indebida en el avance científico del campo de la seguridad de la información.

Con relación a los bloqueos del WhatsApp y su relación con el Marco Civil de Internet, por fin, se plantearon tres hipótesis. La primera entiende que los bloqueos fueron ilegítimos, sea por considerar su impacto desproporcional o por evaluar que las sanciones previstas en el Marco Civil de Internet serían inaplicables. Esa inaplicabilidad podría darse en razón de la imposibilidad técnica de cumplimiento de la orden cuya desobediencia ha ocasionado las sanciones y/o debido a la interpretación de que las sanciones previstas en el Marco Civil de Internet están reservadas a casos de violación de los derechos a la privacidad y a la protección de datos de los usuarios.

La segunda tesis, a su vez, ha entendido que los bloqueos fueron legítimos, una vez que el Marco Civil de Internet prevería la aplicación de las sanciones en la ocurrencia de incumplimiento de la legislación brasileña. Una vez que las órdenes judiciales se fundamentan en la legislación brasileña, su incumplimiento implicaría en violación de nuestro ordenamiento. La tercera, por fin, entendió que la licitud de los bloqueos independería de la redacción del Marco Civil de Internet en sí, pues los magistrados pueden determinar medidas cautelares atípicas en la ausencia de una medida legalmente prevista suficiente para el caso concreto – el llamado poder general de cautela.

Cumple destacar, todavía, el entendimiento común de que las causas concretas de los bloqueos fue un conflicto político entre la empresa Facebook y las instituciones del sistema de justicia criminal brasileño. De ese modo, el episodio tendría dimensiones económicas y políticas que extrapolarían la controversia jurídica específica.

Análisis. Cuanto a la inserción de un mecanismo de acceso excepcional, no es evidente que de la obligación de conducción de interceptaciones, en la hipótesis y términos de la ley, sea posible deducir una aptitud o de alteración en la arquitectura del sistema a fin de tornar la interceptación viable. En lo que se refiere a las implicaciones de la medida, hay consenso científico en el campo de la seguridad informacional sobre la imposibilidad de garantizar que la exploración del mecanismo se realice apenas de forma lícita. Hay aún, indicios empíricos de que regulaciones que debiliten el cifrado causan daños económicos. Por fin, estudios sobre el ambiente político y jurídico brasileño han indicado la ocurrencia de procesos de supresión de las libertades democráticas y uso de la tecnología para viabilidad de medidas autoritarias – fenómeno por veces designado como tecnoautoritarismo.

Cuanto a las alternativas al acceso excepcional, cada una presenta implicaciones distintas. De la obligación judicial del usuario, por medio de sanciones, a la entrega de contraseña de desbloqueo del dispositivo fue recién considerado ilícito por el Superior Tribunal de Justicia en el juicio del RHC nº 580.664 - RJ, con fundamento en la prohibición constitucional a la autoincriminación, lo que implica en la ilicitud de ese expediente. En lo que se refiere al hacking gubernamental, cumple destacar que tales prácticas han sido objeto de críticas de la sociedad civil y por organismos internacionales, que notan su potencial excesivo para el abuso y sugieren que cualesquiera prácticas de esa naturaleza solo se admitan en casos excepcionales, observados requisitos de legalidad, necesidad, proporcionalidad, finalidad legítima, supervisión judicial, entre otros.

Con relación a la propuesta de inserción de usuario o llave fantasma en las comunicaciones, su implementación exige interferencia en el procedimiento de distribución de llaves, lo que implica en la conclusión incontroversa de que la medida representa un debilitamiento del cifrado. De esa manera, sus riesgos son similares a aquellos identificados en el acceso excepcional implementado por medios más convencionales, como la custodia de llaves.

Cuanto al *client-side scanning*, la ausencia potencial de interferencia directa en el sistema cifrado implica que la calibración de la existencia de violación del cifrado es más controvertida. Independientemente de ella, sin embargo, cabe destacar que hay necesaria reducción de la seguridad del sistema como consecuencia de la ampliación de la superficie de ataque, lo que implica en la posibilidad de producción de falsos positivos por medio del comprometimiento de la base de datos utilizada para comparación. Todavía, la posibilidad de alterar la función del sistema representa un riesgo democrático que viene suscitando críticas de la sociedad civil organizada.

En lo que toca a los bloqueos de WhatsApp y su relación con el Marco Civil de Internet, por fin, cumple reiterar primeramente que la suposición de que hay un deber de aptitud a la realización de interceptaciones no solo carece de fundamentación, sino también contraría la jurisprudencia mencionada del Superior Tribunal de Justicia. Cuanto al debate sobre la redacción del Marco Civil de Internet, está pendiente la deliberación del plenario del Supremo Tribunal Federal, pero la tesis de que la aplicación de las sanciones estaría restricta a violaciones de la privacidad y de la protección de datos personales fue aceptada

por los relatores de las acciones sobre el tema. En lo que se refiere al poder general de precaución del juez, el reconocimiento del daño excesivo causado por el bloqueo de la aplicación implica en la ausencia del requisito de proporcionalidad necesario al ejercicio del poder general de cautela.

Por esas razones, se concluye patente que los bloqueos de WhatsApp fueron ilícitos independientemente de lo que delibere el Supremo Tribunal Federal sobre la aplicabilidad de las sanciones previstas en el Marco Civil de Internet. Son ilícitos en razón de la imposibilidad técnica de cumplimiento del orden de entrega de datos en virtud de obstáculo fáctico representado por el cifrado – según entendimiento del STJ. Aunque fueran lícitos, se concluye también que no podrían ser fundamentados en el poder general de cautela del juez en razón del impacto desproporcional en relación a los objetivos deseados– según las órdenes de suspensión de los bloqueos reiteradamente reconocieron.

Conclusiones. El análisis presentado ha evidenciado la complejidad y heterogeneidad de dimensiones y perspectivas que caracterizan las guerras criptográficas. En la imposibilidad de un examen exhaustivo de todos esos aspectos, el mapeo de racionalidades conducido en este estudio ha permitido visibilizar premisas jurídicas y fácticas cuyo mérito es pasible de calibración académica, lo que puede contribuir significativamente para la maduración del debate. Paralelamente, ha demostrado la existencia de racionalidades sociotécnicas y disputas políticas más profundas que subyacen los puntos de vistas de los actores, lo que refuerza la perpetuidad de las guerras criptográficas para más allá de controversias sobre premisas específicas.

1. Introducción

El cifrado, a lo largo de las últimas décadas, ha evolucionado para tornarse una de las herramientas más importantes para garantizar la seguridad en el medio digital. Según se difundió el uso de internet como herramienta para los más variados tipos de servicios, concomitantemente ha aumentado la demanda para que esos servicios fueran prestados de forma segura. Por eso, el uso de cifrado fue progresivamente difundido en la sociedad durante la segunda mitad del siglo XX e inicio del siglo XXI. Algunas de las principales aplicaciones presentes de ese recurso incluyen plataformas de mensajería privada, transacciones electrónicas, servicios bancarios digitales, sistemas de salud y mecanismos de control de tráfico aéreo.

La propagación del uso de cifrado en la sociedad, con todo, no está libre de controversia. En las últimas décadas, autoridades del sector de persecución penal vienen adoptando una retórica crítica al empleo de ciertas aplicaciones cifradas, notablemente el uso de cifrado fuerte[1] para la protección de las informaciones almacenadas o comunicadas por individuos. Para esas instituciones, la masificación del cifrado fuerte en dispositivos personales y plataformas de comunicación se tornó un obstáculo para el ejercicio de sus funciones , pues dificulta o impide la producción de informaciones necesarias a la prevención y represión de la actividad criminosa. Tales actores por veces utilizan el término "oscurecimiento" (*Going Dark*) para designar el alegado fenómeno de que el cifrado tornaría las comunicaciones digitales ilegibles a la autoridad policial, lo que favorecería el cometimiento de ilícitos[2].

En consonancia a esa percepción, tentativas estatales de restringir o limitar el desarrollo y el empleo de cifrado fuerte se observan en diversos países, como Brasil, Estados Unidos, Reino Unido, Rusia y Australia[3]. En general, tales esfuerzos se asocian a la demanda por la introducción de un mecanismo que faculte a la autoridad estatal el acceso a las informaciones cifradas. Esas propuestas frecuentemente encuentran resistencia de especialistas en seguridad de la información y activistas de los derechos digitales, que las contraponen con alegaciones de que tal cambio reduciría la seguridad de los sistemas y sometería a los ciudadanos a potenciales abusos de poder[4].

---

1 Se considera un algoritmo cifrado fuerte o computacionalmente seguro cuando no se puede romper su seguridad en tiempo hábil con los recursos computacionales disponibles en el presente o en el futuro. Ver SCHNEIER, Bruce. **Applied Cryptography**: Protocols, Algorithms, and Source Code in C. 20th Anniversary Edition. New Jersey: John Willey & Sons, 1996, p. 30.

2 Ver BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY (BERKMAN). **Não Entre em Pânico**: Avançando no debate sobre "obscurecimento" (Going Dark). 2018. Tradução por el Instituto de Tecnologia e Sociedade do Rio. Disponible en: https://itsrio.org/wp-content/uploads/2018/10/Dont_Panic_Making_Progress_on_Going_Dark_Debate_PT.pdf. Acceso en 02/08/2021.

3 RODRIGUES, G. R. A controvérsia cifrada: o Clipper e o mito da derrota estatal nas guerras criptográficas dos anos 1990. Em: ALVES, Marco Antônio Sousa. NOBRE, Marcio Rimet. (orgs.). **A sociedade da informação em questão**: o direito, o poder e o sujeito na contemporaneidade. Belo Horizonte: D'Plácido, 2019.

4 RIDER, Karina. The Privacy Paradox: how market privacy facilitates government surveillance. **Information, Communication & Society**. v. 21, n. 10, p.1369-1385, abr. 2017.

Comunmente designadas como guerras criptográficas (*Crypto Wars*), tales controversias asumieron importancia crecente en la agenda de debates sobre políticas de gobernanza de internet en la década de 2010. Las guerras criptográficas evocan consideraciones de seguridad de la información sobre los impactos de arreglos infraestructurales particulares, cuestiones jurídicas referentes a las obligaciones y sanciones aplicables a proveedores de servicios de internet, conflictos políticos entre actores estatales y empresas globales de tecnología y disputas simbólicas sobre los significados del concepto de seguridad y su relación con la privacidad. De esa forma, movilizan las perspectivas de diversos actores, como representantes de la justicia criminal, gestores de empresas privadas de tecnología, activistas de los derechos digitales, especialistas en seguridad de la información, juristas dedicados a las cuestiones tecnológicas, entre otros.

Con el objetivo general de comprender las racionalidades técnicas, jurídicas, políticas y económicas que orientan a los diferentes actores involucrados en la construcción de los debates sobre ese tema en Brasil, el presente trabajo intentó mapear específicamente sus argumentos, creencias y percepciones sobre las relaciones entre cifrado, privacidad, seguridad pública, seguridad de la información y derechos. Para tanto, se realizaron entrevistas cualitativas con más de 40 profesionales especializados o comprometidos con el debate sobre los referidos temas. Los entrevistados fueron seleccionados por medio del método de muestreo en "bola de nieve". Las transcripciones de las entrevistas fueron, a seguir , codificadas y sometidas al análisis cualitativo sistemático de contenido con el auxilio del software Atlas.ti 7.0. Con base en el análisis, sus argumentos y puntos de vista fueron reconstruidos narrativamente y presentados en este trabajo.

La relevancia de esta pesquisa se justifica tanto por la actualidad e importancia política, ya descriptas, de su objeto cuanto por la novedad de su enfoque , una vez que estudios interdisciplinares de impacto que enfoquen empíricamente las diferentes percepciones de los involucrados en la controversia son poco conocidos o inexistentes en la academia nacional. El enfoque jurídico ha predominado en el país, en general por medio de estudios[5] que examinan los bloqueos sufridos por la aplicación WhatsApp a la luz del ordenamiento legal brasileño, analizan y comparan diferentes modelos regulatorios o discuten las relaciones entre el cifrado y los derechos fundamentales. En ese escenario, el trabajo carga el potencial para una contribución innovadora a partir de la cual se podrá extraer una agenda de pesquisa futura que examine de forma profundizada las tesis y percepciones levantadas en este trabajo.

El texto presenta 6 secciones, incluida esta introducción, y dos piezas en anexo (apéndice). En la sección 2, presentamos una breve contextualización de las guerras criptográficas en

5 Ver, por ejemplo, KURTZ, Lahis P.; MENEZES, Victor. A.. Entre o direito e a força na sociedade da informação: bloqueio judicial do WhatsApp e ADI nº 5.527. In: Fabrício Bertini Pasquot Polido; Lucas Costa dos Anjos; Luiza Couto Chaves Brandão. (Org.). **Tecnologias e conectividade**: direito e políticas na governança das redes. 1ed. Belo Horizonte: 2018, v. 1, p. 15-30.; CARVALHO, Thaís B.. **O bloqueio judicial do WhatsApp no território brasileiro no contexto do Estado Democrático de Direito.** 2017. 69 f. Monografía de graduación en el curso de Derecho- Universidade Federal de Lavras, Lavras, 2017; ABREU, Jacqueline S.. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. de Políticas Públicas**, Brasília, v. 7, nº 3, 2017 p. 24-42.; DONEDA, Danilo. MACHADO, Diego. (coords.) **A criptografia no direito brasileiro**. São Paulo: Thompson Reuters - Revista do Tribunais, 2019.

los Estados Unidos y en Brasil, recordando algunos de los procesos y episodios históricos que marcaron la historia del debate en esos contextos. En la sección 3, detallamos la metodología de la pesquisa, elaborando de forma pormenorizada los procesos de selección de los entrevistados, realización de las entrevistas y codificación y análisis de los datos.

En la sección 4, presentamos los resultados de la pesquisa, indicando las percepciones de los entrevistados sobre los siguientes temas: i) acceso excepcional en sistemas cifrados para persecución penal; ii) posibles alternativas para acceso de las autoridades al contenido descifrado sin interferencia directa en el cifrado, como también sus riesgos; iii) evaluación fáctica y normativa sobre el ambiente reglatorio nacional referente al cifrado; iv) opinión sobre los bloqueos de WhatsApp en Brasil y su relación con el Marco Civil de Internet.

A continuación, en la sección 5, los resultados son discutidos por los autores, considerando aspectos contextuales y referencias importantes para el debate. Por fin, se presentan las conclusiones en la última sección, seguidas de los apéndices - donde se encuentran informaciones adicionales sobre la trayectoria metodológica de la pesquisa.

2. Contexto - las Guerras Criptográficas

Según la evolución de las técnicas cifradas, se tornó cada vez más evidente la aplicabilidad estratégica de esa tecnología para la confección de herramientas de diversas naturalezas – incluso para aplicaciones militares –, lo que, a su vez, ha valorizado la cifrado a los ojos de gobiernos alrededor del mundo. Concomitantemente, el avance técnico en esa área del conocimiento, combinado con la perspectiva de exportación y facilitación del acceso a técnicas avanzadas de cifrado para países terceros y hasta mismo para la sociedad civil, motivaron un proteccionismo por parte de los gobiernos que detenían conocimientos más avanzados en el área de cifrado.[6] [7]

Esas acciones proteccionistas son justamente lo que se entiende por Guerras Criptográficas. En líneas generales, fueron embates entre los sectores público y privado, en los cuales el Estado buscaba interponer barreras a la masificación del uso del cifrado por empresas que, conocedoras del apelo comercial de la tecnología, anhelaban incluirla en sus productos. Tradicionalmente, se enumeran dos ocurrencias principales de esos eventos – al final del siglo XX y a partir de 2013 –, correspondientes a la Primera y

6 FROOMKIN, M. The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. **University of Pennsylvania Law Review**, v. 143, n. 3, p. 709–897, 1995.

7 INMAN, B. R. The NSA perspective on telecommunications protection in the nongovernamental sector. Cryptologia, v. 3, n. 3, 129 - 135, 1979.

a la Segunda Guerras Criptográficas[8]. Importa destacar, con todo, el entendimiento actual de que las Crypto Wars no se trataron de eventos aislados y compartimentados, sino de puntos de destaque en un contexto de perene conflicto involucrando intereses estatales, empresariales y civiles.[9] A continuación , se presentará un breve resumen de los principales eventos que marcaron ese conflicto y sus principales hitos a fin de contextualizar la lectura.

2.1. Guerras criptográficas en el siglo XX

Hubo dos episodios principales que sintetizan la primera etapa de las Guerras Criptográficas, que tiene raíces en la década de 70 y duró aproximadamente hasta el final de la década de 1990.

Durante la II Guerra Mundial, se utilizaban mensajes cifrados para permitir la comunicación por radio entre fuerzas aliadas, impidiendo que estas fueran comprendidas por el enemigo. En ese escenario, se empleaban esfuerzos para descifrar las comunicaciones enemigas y obtener una ventaja estratégica. Aproximadamente en ese período – como consecuencia de su enorme utilidad bélica –, el cifrado pasó a ser considerado por el gobierno estadounidense como análogo a la munición militar.

En ese contexto, el primer momento de las Crypto Wars consistió en una serie de tensiones relacionadas a los intentos de los EUA de restringir la diseminación doméstica y exterior de la cifrado. En el plan externo, eso se dio por medio de la interposición de barreras estrictas para la exportación de técnicas cifradas. Categorizada como forma de armamento, el cifrado fue inserida entre los ítems protegidos por las legislaciones estadunidenses relativas a la exportación de equipo bélico – la *International Traffic in Arms Regulations* y el *Arms Export Control Act*[10], ambas normas de 1976.

En el plan doméstico, a su vez, la actuación de NSA se volvía hacia inhibir la difusión del cifrado fuerte en el sector privado y en la sociedad civil. En ese punto, se destaca el intento gubernamental de determinar el algoritmo criptográfico a ser utilizado por el sector privado, el *Data Encryption Standard* (DES), desarrollado por NSA y por la Agencia

8 A pesar de la enumeración usual de las Guerras Criptográficas en dos instancias, el historiador y criptólogo Craig Jarvis argumenta en favor del reconocimiento de como mínimo uno más de esos eventos. Según Jarvis, la Primera Guerra Criptográfica habría ocurrido entre los años de 1966 y 1981, englobando eventos como la creación del primer algoritmo cifrado aprobado por el gobierno de los EEUU(el llamado DES, o "*Data Encryption Standard*"), que fue acusado por diversos criptólogos de haber sufrido alteraciones en su funcionamiento para permitir acceso extraordinario de NSA a las comunicaciones cifradas. La Primera Guerra Criptográfica, según el autor, también habría incluido el intento del gobierno estadounidense de impedir la publicación de la obra *The Codebreakers*, de David Kahn. Para más informaciones, consultar: JARVIS, Craig. **Crypto Wars**: The Fight for Privacy in the Digital Age: A Political History of Digital Encryption. CRC Press, 2020.

9 AULA 4 - Criptografia: experiências regulatórias e debates internacionais con Diego Canabarro. Belo Horizonte: Instituto Iris, 2021. (39 min.), son., color. Disponible en: https://youtu.be/EDaI5_z-hBo?t=2200. Acceso el: 25 ago. 2021.

10 ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, nº 3, 2017, p. 24-42. p. 29.

Nacional de Patrones[11]. En 1977, el gobierno federal del país seleccionó una versión revisada de ese patrón, el algoritmo LUCIFER, desarrollado por IBM, como patrón nacional. La implementación del LUCIFER/DES fue objeto de críticas de la comunidad técnica y del sector privado, pues imponía un límite severo sobre el tamaño de las llaves cifradas[12]. Además, críticos sospechaban que pudiera haber un "backdoor" – una vulnerabilidad inserida a propósito en el sistema – en el algoritmo.

La década de 1970, todavía, fue marcada por otro evento llave: la publicación del artículo *New directions in cryptography* por los investigadores Whitfield Diffie y Martin Hellman en la revista *IEEE Transactions on Information Theory* en 1976[13]. Hoy conocido como cifrado de llave pública o cifrado asimétrico, el método de distribución de llaves desarrollado por la pareja permitía el desarrollo de sistemas que dispensaban cualquier tercero de confianza. Conjugados, la resistencia civil a LUCIFER/DES y el advenimiento del cifrado asimétrico señalaban una menaza al control de NSA sobre el cifrado. Preocupaciones de esa naturaleza ya eran expresadas por los liderazgos de la agencia en el final de la década. En 1979, por ejemplo, Bobby Inman, en aquella época director de la agencia, escribía acerca de la materia[14]:

> Desde la perspectiva de NSA, el núcleo del problema es que preocupaciones mayores sobre la protección de las telecomunicaciones en el sector no-gubernamental implica mayor conocimiento y discusión pública sobre técnicas de protección de las comunicaciones. La principal de esas técnicas es, por supuesto, el cifrado. Hay un peligro bastante real y crítico de que discusión pública irrestricta sobre cuestiones cifradas perjudicará seriamente la habilidad de ese gobierno en conducir inteligencia de señales y la capacidad de ese gobierno para desempeñar su misión de proteger informaciones de seguridad nacional de exploración hostil (énfasis de os autores de este estudio, traducción libre).

El segundo punto de inflexión ocurrió años más tarde, en la década de 1990 – aunque durante ese intervalo la presión de los EEUU contra la diseminación del cifrado haya permanecido constante. El marco inicial de esa nueva fase de las guerras criptográficas

11 LIU, H. Inside the Black Box: Political Economy of the Trans-Pacific Partnership's Encryption Clause. **Journal of World Trade**, v. 51, n. 2, p. 309 - 334, 2017.

12 El patrón propuesto originalmente permitiría llaves criptográficas de 100 bits, pero NSA exigió que ese número fuera reducido para 56. Una vez que llaves menores se pueden romper más fácilmente por medio de ataques de búsqueda exhaustiva de llave, en los cuales se recorre rápidamente todas las llaves posibles, críticos pasaron a ver LUCIFER/DES como desarrollado para que la llave fuera "larga lo suficiente para frustrar observadores disimulados de corporaciones, pero suficientemente pequeña para que la rompiera NSA". Ver FROOMKIN, M. The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. **University of Pennsylvania Law Review**, v. 143, n. 3, p. 709–897, 1995, p. 735, traducción libre.

13 DIFFIE, Whitfiead. HELLMAN, Marin. New directions in cryptography. **IEEE Transactions on Information Theory**, 22, 644-654.

14 INMAN, B. R. The NSA perspective on telecommunications protection in the nongovernamental sector. **Cryptologia**, v. 3, n. 3, 129 - 135, 1979.

ocurrió en 1993, cuando se propuso el *Escrowed Encryption Standard* (patrón de cifrado bajo custodia, en traducción libre). Como el nombre sugiere, se trató de una propuesta por medio de la cual el gobierno estadounidense pretendía estandarizar la venta de cifrado para terceros, condicionándola a la custodia de las llaves cifradas de sus comunicaciones por agentes de investigación pública[15].

Se alcanzaría ese objetivo a través de la implementación de los llamados "Clipper Chip" y "Capstone Chip" respectivamente en teléfonos y computadoras – coprocesadores que encriptarían las comunicaciones realizadas por los usuarios, pero guardarían una copia de las llaves cifradas en custodia de una entidad tercera considerada confiable por los proponentes del patrón. De esa forma, a través de un *backdoor*, las entidades investigativas estadounidenses podrían tener acceso a todo contenido de las comunicaciones encriptadas de los usuarios.[16]

El patrón propuesto fue blanco de severas críticas por parte del sector empresarial, consciente de que la comercialización de dispositivos que contenían Clipper y Capstone estaba destinada a sufrir delante de la competencia internacional de empresas extranjeras no sometidas a esa exigencia legal. Al mismo tiempo, hubo gran movilización contraria al *Escrowed Encryption Standard* por parte de la comunidad técnico-científica y de la sociedad civil, que respectivamente apuntaban hacia los riesgos de seguridad del modelo y los ataques a las libertades civiles que él representaba.[17]

Paralelamente a la presión contraria a la utilización del Clipper y del Capstone, el lanzamiento del PGP (*Pretty Good Privacy*) en 1991 fue fundamental para la caída del *Escrowed Encryption Standard*. Se trataba de un software gratuito de cifrado de llave pública, que sirvió como exposición inicial de la población civil a los algoritmos cifrados realmente seguros. Su creador, Phil Zimmermann, fue sometido a años de investigación por parte de las autoridades estadounidenses, pero eventualmente considerado inocente, mediante el reconocimiento de que los métodos utilizados para la diseminación del software eran protegidos por la legislación para la libertad de expresión en los EEUU.[18]

Durante la década de 1990, se realizaron diversas audiencias públicas acerca del tema, que contribuyó enormemente para la diseminación pública del debate sobre cifrado, seguridad y privacidad. Los debates culminaron en la derrocada pública de propuestas como el Clipper y Capstone.

La derrota pública del *Escrowed Encryption Standard*, las presiones populares por la

15 FROOMKIN, Michael. The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. **University of Pennsylvania Law Review**, v. 143, n. 3, p. 709–897, 1995.

16 SINGH, Simon. **The Code Book**: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: First Anchor Books, 2000. p. 234-235.

17 ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, nº 3, 2017, p. 24-42.

18 SINGH, Simon. **The Code Book**: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: First Anchor Books, 2000. p. 226-237.

liberación del uso de cifrado fuerte y segura en los EEUU y la competencia internacional por parte de países que también estaban desarrollando sus técnicas criptográficas culminaron, al final del milenio, en la relajación de las barreras creadas desde los años 70 para la comercialización de esa tecnología. En ese período, se observó un crecimiento considerable en el uso de servicios cifrados, que pasaron a ser empleados en gran escala por la población civil.

Eso no significa que las guerras criptográficas se hayan simplemente encerrado al fin del siglo XX. Como argumenta la socióloga Karina Rider[19], la primera década del siglo XXI fue marcada por la consolidación de los programas de vigilancia masiva conducidos por el sector de inteligencia de los EEUU con la cooperación de diversas empresas de tecnología. El Bullrun, uno de los principales programas en cuestión, visaba específicamente asegurar que NSA continuaría apta a acceder a comunicaciones cifradas fuera por el debilitamiento intencional de los algoritmos o por la manipulación del mercado cifrado. La década de 2010 se puede comprender como un período de ocultamiento de las guerras criptográficas, que pasan a ocurrir lejos de los focos del debate público.

2.2. Guerras criptográficas actuales (2013 - presente)

La llamada Segunda Guerra Criptográfica tuvo inicio aproximadamente en el año de 2013, a partir de las denuncias de Edward Snowden. El exintegrante tanto de la Agencia Central de Inteligencia (CIA) como de la Agencia Nacional de Seguridad de los EEUU (NSA) ha denunciado las prácticas de ciber-vigilancia adoptadas por el gobierno estadounidense, lo que inició un movimiento global de busca por mecanismos de seguridad verdaderamente efectivos.

Un segundo evento notorio ocurrió en 2015: se trata del caso *Apple vs. FBI*. El proceso ocurrió en virtud del cifrado total de disco utilizada en los celulares de la fabricante. El FBI buscaba por medios judiciales como una forma de obligar a la empresa auxiliar en el desbloqueo de un iPhone 5C, cuyos contenidos estaban protegidos con cifrado fuerte, y que había sido utilizado por un individuo investigado en virtud del ataque terrorista de San Bernardino, en California. La empresa se recusó a auxiliar el órgano de investigación, alegando que la implementación de un *backdoor* en su sistema operacional resultaría en perjuicios para la seguridad de toda la base de usuarios de la plataforma iOS. A pesar del FBI haber desistido del proceso judicial, por haber contornado el cifrado del dispositivo por medios diversos y accedido a las informaciones pretendidas, el caso *Apple vs. FBI* fue utilizado como ejemplo para motivar un aumento en la presión ejercida por autoridades investigativas contra técnicas de cifrado fuerte[20].

19 RIDER, Karina. The Privacy Paradox: how market privacy facilitates government surveillance. **Information, Communication & Society**. v. 21, n. 10, p.1369-1385, abr. 2017.

20 MITCHELL, Bonnie et al. **Going Dark**: Impact to Intelligence and Law Enforcement and Threat Mitigation. US Department of Homeland Security. Office of Intelligence and Analysis. 2017. p. 14

Esa presión está muy bien ilustrada por el discurso[21] proferido en 2014 por el entonces director del FBI, James Comey, que contribuyó significativamente para la difusión pública del concepto de "*Going Dark*". Se trata de la idea de que los mecanismos modernos de seguridad y privacidad representan un "oscurecimiento" de las herramientas investigativas estatales y representan, por lo tanto, un obstáculo al combate al crimen cibernético, al terrorismo y a la efectuación de la justicia.

Going Dark fue posteriormente mencionado en un informe[22] publicado en 2017 por el Gabinete del Director de Inteligencia Nacional de los EEUU (ODNI). En el documento, se presentan posibles soluciones para la cuestión del oscurecimiento, con recomendaciones que incluyen el fortalecimiento de las llamadas actividades de *hacking* gubernamental, como también de alianzas técnicas con representantes del sector privado, a fin de posibilitar a las autoridades investigativas el acceso a los medios de prueba considerados necesarios para la persecución penal de posibles infractores.

La narrativa del oscurecimiento eventualmente ha ganado repercusión internacional y ha motivado la creación de legislaciones que buscan la debilitación de técnicas de cifrado fuerte en diversos países. Notadamente, se puede citar la aprobación del *Telecommunications and Other Legislation Amendment* en Australia en 2018, que determina, entre otros, que proveedores de servicios de comunicación faciliten el acceso de las autoridades estatales a datos, incluso cifrados, por medio de mandados de asistencia técnica o acceso a informaciones.[23]

La India recientemente también se ha tornado un ejemplo de país cuya legislación presenta posibles obstáculos para el uso de técnicas criptográficas. Esto porque en 2021 se aprobó la emenda a las reglas aplicables a los medios digitales en el país, con obligaciones de rastreo de los perpetuadores originales de los contenidos publicados. En ese sentido, hay recelo de que aplicaciones de mensajería instantánea con cifrado de punta-a-punta para proteger las comunicaciones de sus usuarios puedan tener la seguridad de sus sistemas perjudicada para atender a las exigencias legales.[24] [25]

21 COMEY; James B. **Going Dark:** Are Technology, Privacy, and Public Safety on a Collision Course? Oct. 2014, discurso realizado en Brookings Institution. [Online]. Disponible en https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course. Acceso el: 02 ago. 2021.

22 MITCHELL, **Bonnie et al. Going Dark:** Impact to Intelligence and Law Enforcement and Threat Mitigation. 2017.

23 Stilgherrian. **The Encryption Debate in Australia:** 2021 Update. 2021.

24 GROVER, Gurshabad; RAJWADE, Tanaya; KATIRA, Divyank. The Ministry And The Trace: Subverting End-To-End Encryption, 14 NUJS Law Review. 1(2021). p. 2-6. Disponible en http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption/. Acceso em: 02 ago. 2021.

25 RAY, Trisha. The Encryption Debate in India: 2021 Update. 2021.

2.3. Las guerras criptográficas en Brasil

2.3.1. Los bloqueos de WhatsApp en el país

De forma similar a lo que ocurrió en los EEUU y otros países alrededor del globo, el debate cuanto al oscurecimiento de la justicia también ha ganado fuerza en Brasil. Los cuatro intentos de bloqueo de la aplicación WhatsApp entre los años de 2015 y 2016 fueron algunas de las primeras instancias de ese debate en el país.

En febrero de 2015, en la Comarca de Teresina, Piauí, el juez Luiz de Moura Correia concedió el pedido, realizado por el Núcleo de Inteligencia de la Policía Civil del Estado de Piauí, de suspensión de las actividades de la empresa en Brasil. En nota, el magistrado afirmó que la medida ocurrió "en razón de reiterados no cumplimientos de órdenes judiciales emanadas de este Juicio, en diversos procedimientos que apuran crímenes de la más elevada gravedad"[26]. La orden fue suspendida en el mismo día por el Tribunal de Justicia de Piauí[27], que la consideró desproporcional y dañosa a los usuarios, además de entender que existían medios menos gravosos de investigación. El bloqueo no se llegó a concretar.

El segundo bloqueo ocurrió en diciembre de aquel mismo año, determinado por la 1ª Vara Criminal de São Bernardo do Campo, São Paulo y suspendido cerca de 12 horas después de su inicio[28]. Según relata la liminar de suspensión del bloqueo[29], la empresa no cumplió comando judicial de interceptación de comunicaciones telemáticas de tres personas investigadas en el contexto de apuración de la práctica de tráfico de drogas, lo que suscitó la aplicación de multa diaria y, subsecuentemente, el bloqueo de la aplicación por 48 horas. El Tribunal de Justicia del Estado de São Paulo suspendió el bloqueo por entender que la medida violaba el principio de la proporcionalidad y que existirían medios menos gravosos de coerción de la empresa, como la elevación del valor de la multa.

Después de los dos primeros bloqueos, WhatsApp anunció el día 05 de abril de 2016 la implementación del cifrado de punta-a-punta[30], afirmando que "todas los mensajes,

26 BRASIL. Central de Inquéritos da Comarca de Teresina. **Nota**. Juiz Luiz de Moura Correia. Teresina, 26 fev. 2015. Disponible en: http://s2.glbimg.com/MdNVliNDOaF45o27HM8_tsG3wlI=/s.glbimg.com/jo/g1/f/original/2015/02/26/nota_juiz_whatsapp_ok.jpg. Acceso em: 29/07/2021.

27 BRASIL. Tribunal de Justiça do Estado do Piauí. **Mandado de Segurança nº 2015.0001.001592-4**. Rel. Des. Raimundo Nonato da Costa Alencar. Teresina, 26 fev. 2015. Disponible en: <http://www.migalhas.com.br/arquivos/2015/2/art20150227-03.pdf> Acceso el : 29/07/2021.

28 BARIFOUSE, R.; DUARTE, F.; BARRUCHO, L. G. Liberação do WhatsApp não encerra polêmica disputa com Justiça brasileira. **G1**. Tecnologia e Games. Disponible en: http://g1.globo.com/tecnologia/noticia/2015/12/liberacao-do-whatsapp-nao-encerra-polemica-disputa-com-justica-brasileira.html. Acceso el: 29/07/2021.

29 BRASIL. Tribunal de Justiça do Estado de São Paulo. **Mandado de Segurança nº 2271462-77.2015.8.26.0000**. Decisão liminar. Rel. Des. Xavier de Souza. São Paulo, 17 dez. 2015. Disponible en: http://www.omci.org.br/m/jurisprudencias/arquivos/2015/tjsp_22714627720158260000_17122015.pdf. Acceso el: 29/07/2021.

30 WHATSAPP INC. **Blog do WhatsApp**. Criptografia de Ponta-a-Ponta. 05 abr. 2016. Disponible en: https://blog.whatsapp.com/end-to-end-encryption. Acceso el: 30/07/2021

fotos, vídeos, archivos y mensaje s de voz" trocadas entre usuarios que utilizasen las últimas versiones de la aplicación estarían protegidas por el cifrado, a partir del protocolo criptográfico Signal.

Posteriormente en aquel mes ocurrió el tercer caso, cuando la vara criminal de la Comarca de Lagarto, Sergipe, determinó, el 26 de abril, la suspensión de la aplicación por 72 horas en razón de nuevo no cumplimiento de orden judicial de entrega de datos personales de usuarios de la aplicación[31]. La orden mencionó los artículos 3, 10, 11, 12, 13 y 15 del Marco Civil de Internet como sus fundamentos. El bloqueo fue suspendido por el Tribunal de Justicia de Sergipe[32], que entendió que la suspensión de los servicios generó "caos general en todo el territorio", como también no era posible afirmar "que las informaciones podrían ser provistas por WhatsApp o que estas podrían desencriptar para servir a la Justicia".

Por fin, el cuarto bloqueo fue determinado por la 2ª vara criminal de la Comarca de Duque de Caxias, Rio de Janeiro, también por no cumplir orden judicial de rotura de sigilo e interceptación telemática de mensajes. Según relata la decisión[33], la orden fue respondida con un e-mail redactado en inglés, lo que fue interpretado por la magistrada como una señal de desconsideración de la autoridad nacional. El documento hace referencia a los artículos 7, 10 y 11 del MCI, al art. 139, IV, del Código de Proceso Civil y al art. 3º del Código de Proceso Penal. El bloqueo fue suspendido por el Supremo Tribunal Federal, que entendió [34] que el bloqueo violaba el precepto fundamental de la libertad de expresión como también configuraba medida desproporcional. Así, con base en el poder general de cautela, revertió la decisión.

2.3.2. La cifrado en el Supremo Tribunal Federal: la ADI 5527 y la ADPF 403

Los diversos episodios de bloqueo del WhatsApp en Brasil generaron gran repercusión entre los diferentes sectores de la sociedad: desde los usuarios en general, que se vieron impactados por la inaccesibilidad del servicio durante la vigencia de esas órdenes judiciales, hasta la comunidad jurídica y técnico-científica, que comentaron extensamente sobre la legitimidad o no de los comandos de bloqueo.

Concomitantemente a la discusión acerca de los casos, se enjuiciaron delante el Supremo

31 BRASIL. Juízo de Direito da Vara Criminal da Comarca de Lagarto. **Processo nº 201655090143**. Decisão. Juiz Marcel Maia Montalvão. Lagarto, Sergipe, 26 abr. 2016.

32 BRASIL. Tribunal de Justiça do Estado de Sergipe. **Mandado de Segurança nº 201600110899**.Decisión liminar. Rel. Des. Ricardo Múcio Santana de Abreu Lima. Aracaju, 3 mai. 2016. Disponible en: <http://www.omci.org.br/m/jurisprudencias/ arquivos/2016/tjse_201600110899_03052016.pdf> Acceso em: 2 nov. 2016.

33 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Inquérito Policial nº 062-00164/2016**. Juíza Daniela Barbosa Assumpção de Souza. Duque de Caxias, RJ, jul. 2016. Disponible en: <https://drive.google.com/file/d/0Bw3seZUv__5ubnFudjUwMm9OZGc/view>. Acceso el: 30/07/2021

34 BRASIL. Supremo Tribunal Federal. **Medida cautelar de arguição de descumprimento de preceito fundamental**. Decisão liminar. Rel. Min. Ricardo Lewandowski. Brasília, 19 jul. 2016. Disponible en: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403MC.pdf. Acceso el: 30/07/2021.

Tribunal Federal la Petición de No Cumplimiento de Precepto Fundamental (ADPF) nº 403[35] y, poco después, la Acción Directa de Inconstitucionalidad (ADI) nº 5527[36]. El objetivo de esas acciones fue, en resumen, cuestionar la validad jurídica de las órdenes de bloqueo do WhatsApp delante la instancia máxima del Poder Judiciario brasileño, para que la decisión cree un mecanismo jurisprudencial que impida nuevas órdenes de bloqueo de la plataforma.

Enjuiciada después de la segunda determinación de bloqueo de la plataforma, la ADPF 403 sostiene que órdenes judiciales de esa naturaleza violan el precepto fundamental de la libertad de comunicación– enunciado en el art. 5º, IX, de la Constitución Federal. Además, se alega que hubo también un no cumplimiento del principio de la proporcionalidad, llévese en cuenta que las órdenes de bloqueo – relativas a casos aislados e individualizados que tramitan en el Judiciario – resultan en la inaccesibilidad de la plataforma por toda la sociedad brasileña.

La ADI 5527, a su vez, busca declarar la inconstitucionalidad de los artículos del Marco Civil de la Internet (Ley nº 12.965/2014) utilizados para fundamentar las órdenes judiciales de bloqueo del WhatsApp. Más específicamente, se argumenta a favor de la declaración de inconstitucionalidad de los incisos III y IV del art. 12 del Marco Civil, que se refieren a las sanciones de suspensión temporal y de prohibición de las actividades de proveedores de aplicación por falla en ofrecer contenidos de comunicaciones privadas requeridas en juicio (según previsto en el art. 10, §2º, de la misma ley).Además, ADI busca limitar los efectos del art. 10, §2º, para que ese dispositivo legal se aplique apenas a casos de persecución penal – y no para no cumplimiento de órdenes judiciales en ambiente civil, como ocurrió con los bloqueos de WhatsApp.

Debido a la similitud de temas tratados en ambas acciones, se realizó una audiencia pública conjunta en 2017, para que se recogieran informaciones sobre cuestiones técnicas y prácticas involucradas en las controversias de los bloqueos de la plataforma. Durante dos días, diversas entidades, representando los intereses de los sectores técnico-científico, gubernamental, tercer sector y sector empresarial, fueron escuchadas por los Ministros relatores de ambas las acciones de control concentrado de constitucionalidad[37] Las decisiones proferidas por el STF en cada uno de esos procesos serán paradigmáticas para el futuro de las comunicaciones protegidas por cifrado fuerte en Brasil. A causa de la complejidad y sensibilidad del tema, con todo, tanto la ADPF 403 como la ADI 5527 están todavía aguardando juicio definitivo, en razón de vista solicitada por el Ministro Alexandre de Moraes en mayo de 2020, pero pronunciamientos y votos importantes ya fueron proferidos por sus relatores.[38]

35 BRASIL. Supremo Tribunal Federal. **ADPF 403**. Relator: Edson Fachin. Brasília, DF. Disponible en: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500. Acceso el: 06 ago. 2021.

36 BRASIL. Supremo Tribunal Federal. **ADI 5527**. Relatora: Rosa Weber. Brasília, DF. Disponible en: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282. Acceso el: 06 ago. 2021.

37 ABREU, Jaqueline. **Audiência Pública sobre Criptografia e Bloqueios do WhatsApp:** argumentos diante do STF. 26/06/2017. Bloqueios.info . Disponible en <http://bloqueios.info/pt/audiencia-publica-sobre-criptografia-e-bloqueios-do-whatsapp-argumentos-diante-do-stf/ >, acceso el 02 ago 2021.

38 CANTO, Mariana. RAMIRO, André. REAL, Paula C. **Criptografia no STF:** O que dizem os votos de Rosa Weber e Edson

La Ministra Rosa Weber, relatora de la ADI 5527, por ejemplo, ya se ha pronunciado en sentido de que las previsiones de los incisos III y IV del art. 12 del Marco Civil se destinan al no cumplimiento de obligaciones de protección de registros, datos personales y comunicaciones – y no para el no cumplimiento de órdenes judiciales.

Además, defendió no existir una dicotomía entre la busca por la seguridad pública y el derecho a la privacidad – como costumbran alegar los órganos investigativos y los defensores de la idea del oscurecimiento. La Ministra, en ese sentido, observó que medidas de acceso excepcional a comunicaciones cifradas representan violaciones a los derechos a la libertad de expresión y a la protección al sigilo de las comunicaciones. Además, que la debilitación del cifrado representaría un retroceso para el país y sería un "presente para regímenes autoritarios y criminosos".

El Ministro Edson Fachin – relator de la ADPF 403 –, a su vez, defendió la idea de que derechos digitales deben ser tan completos como los derechos que la población detiene en el medio offline y representan derechos fundamentales de los brasileños. En ese sentido, el Ministro argumentó que la cifrado es un medio de asegurarse la protección de derechos que son esenciales para la vida pública en una sociedad democrática. Por eso, sería contradictorio reducir la seguridad en la internet en nombre de la seguridad pública. Fachin también ha argumentado que la implementación de *backdoors* o demás vulnerabilidades sistémicas en algoritmos cifrados – aunque apenas destinados a autoridades investigativas –, representaría una debilitación de la seguridad de esos sistemas de forma universal. Eso porque actores terceros mal intencionados también tendrían acceso a esas herramientas, colocando en riesgo la totalidad de los usuarios de los servicios afectados.

2.3.3. El cifrado delante de la ley brasileña y otros conflictos recientes

La legislación brasileña vigente, en su mayoría, no hace mención específica a técnicas criptográficas. Eso no significa, con todo, que no exista un incentivo perceptible para la implementación de esa tecnología en sistemas digitales.

El Marco Civil de Internet, por ejemplo, promueve el uso de medidas técnicas compatibles con los patrones internacionales para la preservación de la estabilidad, seguridad y funcionalidad de la red (art. 3º, V). El decreto reglamentar de esa ley (Decreto nº 8.771/2016), a su vez, enuncia el cifrado como una de las soluciones tecnológicas posibles y recomendadas para gestionar registros digitales de manera segura (art. 13, IV).

Ya más recientemente, la Ley General de Protección de Datos Personales (Ley nº 13.709/2018) trató de la adopción de patrones técnicos adecuados para garantizar la seguridad y salvaguarda de datos personales que estén bajo la tutela de agentes

Fachin e o que podemos aprender com eles. Disponible en https://ip.rec.br/2020/06/22/criptografia-no-stf-o-que-dizem-os-votos-de-rosa-weber-e-edson-fachin-e-o-que-podemos-aprender-com-eles/. Acceso el 02 ago 2021.

de tratamiento. Enunciados en ese sentido se pueden encontrar , por ejemplo, entre los principios orientadores de la protección de datos en Brasil (art. 6º, VI y VII), en los requisitos legales para seguridad y sigilo de datos (arts. 46, 47), en los dispositivos que prevén una desaceleración de las penalidades aplicadas en incidentes de protección de datos, cuando esté comprobado que los agentes de tratamiento involucrados adoptaron patrones técnicos, administrativos y operacionales adecuados para evitar el incidente (arts. 48, § 3º, y 52, §1º, VIII), entre otros.

En lo que se refiere específicamente al uso de cifrado en aplicaciones de mensajería privada, el Superior Tribunal de Justicia ya decidió más de una vez en defensa de la encriptación de datos utilizada en esos servicios. En ese sentido se pronunciaron la Tercera Sección [39] y la Quinta Turma[40] del STJ, que no consideraron razonable la imposición de multa a proveedores de mensajería privada por no cumplimiento de orden judicial a causa de imposibilidades técnicas inherentes a la tecnología empleada.

A pesar de esos enunciados legales y de los entendimientos jurisprudenciales recientes, se observa en el Legislativo nacional la tramitación de una serie de proyectos de ley que, de una forma o otra, buscan relativizar el derecho al uso de cifrado fuerte en Brasil. Se pueden mencionar, a título de ejemplo, el PL nº 5.285/2009, el PL nº 9.808/2018, el PL nº 11.007/2018 y el PL nº 2.418/2019. A pesar de disponer sobre medidas legislativas distintas, todos esos proyectos tienen en común el objetivo de restringir o debilitar el derecho al uso de técnicas criptográficas en Brasil – sea por medio de la criminalización expresada del acto o incluso por medio de la institucionalización de mecanismos de acceso excepcional del Estado a comunicaciones cifradas.[41]

No obstante, la importación de la narrativa de *Going Dark* para Brasil tuvo todavía otras repercusiones para el escenario nacional. En 2019, fue organizado por el entonces Ministro de Justicia y Seguridad Pública, Sérgio Moro, el I Simposio Going Dark Brasil.[42] El evento se destinó a la exposición de las dificultades vivenciadas por órganos investigativos estatales en virtud de técnicas criptográficas y terminó con la firma de una declaración[43] por representantes de 13 países. En el documento, los avances tecnológicos recientes – como cifrado y técnicas semejantes– se presentan como técnicas utilizadas por

39 BRASIL. Superior Tribunal de Justiça. **Terceira Seção afasta multa contra empresa que alega impossibilidade de interceptar mensagens criptografadas.** 30/12/2020. Disponible en < https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/30122020-Terceira-Secao-afasta-multa-contra-empresa-que-alega-impossibilidade-de-interceptar-mensagens-criptografadas.aspx >, acceso el 03 ago 2021.

40 BRASIL.Superior Tribunal de Justiça. **Criptografia em aplicativo de mensagem não permite multa cominatória, decide Quinta Turma.** 24/06/2021. Disponible en <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/24062021-Criptografia-em-aplicativo-de-mensagem-nao-permite-multa-cominatoria--decide-Quinta-Turma.aspx>, acceso el 03 ago 2021.

41 Confira: RAMIRO, André. CANTO, Mariana. REAL, P. C. et al. **O Mosaico Legislativo da Criptografia no Brasil: Uma Análise de Projetos de Lei**. IP.Rec. Disponible en<https://ip.rec.br/wp-content/uploads/2020/08/O-mosaico-legislativo-da-criptografia-no-Brasil-uma-an%C3%A1lise-de-Projetos-de-Lei-1.pdf >, acceso el 04 ago 2021.

42 BRASIL. Ministério da Justiça e Segurança pública. **Simpósio sobre Going Dark termina com declaração de 13 países.** Disponible en <https://www.justica.gov.br/news/collective-nitf-content-1550010028.2>, acceso el 03 ago 2021.

43 BRASIL. **Declaração do Going Dark Brasil.** Disponible en <https://www.justica.gov.br/news/collective-nitf-content-1550010028.2/documentos/declaracao-do-going-dark-brasil.pdf> acceso el 04 ago 2021.

terroristas y criminosos para impedir el poder investigativo estatal, que motivarían , por lo tanto, la acción conjunta de la comunidad internacional para prevenir abusos en ese sentido.

Se menciona, aún, el así llamado "Paquete Anticrimen", también idealizado por el ex-Ministro Sérgio Moro y promulgado en la forma de la Ley nº 13.964/2019. En su texto original, la regulación preveía la ampliación de los poderes de interceptación de órganos investigativos estatales y presuponía el deber de las plataformas de colaborar para con la persecución penal. De esa forma, el mecanismo dejaba subentendida la extensión de esas obligaciones para proveedores de servicios protegidos por cifrado fuerte.

Más recientemente, el texto preliminar del nuevo Código de Proceso Penal[44] generó controversias a causa de la posible alteración de los mecanismos vigentes de autoridades investigativas a informaciones sigilosas. El proyecto incluye una expansión de los poderes estatales para interceptación de comunicaciones telemáticas. Entre los enunciados previstos, se destaca la obligación de asistencia establecida para proveedores de servicios de telecomunicaciones, según la cual sus proveedores pasarían a tener la obligación legal de liberar los recursos y medios tecnológicos necesarios para su interceptación.

Esos enunciados provocaron recelo en integrantes de la sociedad civil organizada y de la comunidad técnico-científica nacional[45] e internacional[46], por la posibilidad de que se establezca un mecanismo legal para inserción de vulnerabilidades en sistemas cifrados, como supuesto para la conformidad regulatoria de servicios de comunicación que emplean medidas de seguridad de esa naturaleza. Eso, a su vez, puede representar una reducción sistémica en la confiabilidad y seguridad proporcionada por esos servicios, en pro de alegados beneficios a la seguridad nacional.

Se percibe, por lo tanto, que la importación de la narrativa del oscurecimiento para el contexto brasileño, como también la existencia de una guerra institucional contra la cifrado – una Guerra Criptográfica –, representan tensiones y amenazas actuales para el futuro de esa tecnología en Brasil.

44 AGÊNCIA CÂMARA DE NOTÍCIAS. Relatório preliminar do novo CPP incorpora provas digitais e novas tecnologias ao processo criminal. Relator: Deputado João Campos. 13/04/2021. Disponible en:<https://www.camara.leg.br/noticias/745824-relatorio-preliminar-do-novo-cpp-incorpora-provas-digitais-e-novas-tecnologias-ao-processo-criminal/ >, acceso el 26 ago. 2021.

45 COALIZÃO PELOS DIREITOS NA REDE. Reforma do Código de Processo Penal pode aumentar vigilância e precisa de equilíbrio em questões de tecnologia. 20 de mayo de 2021. Disponible en < https://direitosnarede.org.br/2021/05/20/reforma-do-codigo-de-processo-penal-pode-aumentar-vigilancia-e-precisa-de-equilibrio-em-questoes-de-tecnologia/>, acceso el 25 ago. 2021.

46 Global Encryption Coalition. Brazilian Code of Criminal Procedure reform must not undermine encryption. June 28, 2021. Disponible en < https://www.globalencryption.org/2021/06/brazilian-code-of-criminal-procedure-reform-must-not-undermine-encryption/>, acceso el 25 ago. 2021.

3. Metodología

Esta sección describe la metodología utilizada en la pesquisa. El ítem 3.1. detalla la selección y el perfil de los entrevistados. El ítem 3.2 discute la dinámica de las entrevistas. El ítem 3.3 detalla el procedimiento de codificación y análisis de los datos. El ítem 3.4. resalta las limitaciones de la metodología adoptada.

3.1. Selección de los entrevistados

La selección de entrevistados se realizó por el método de muestreo en "bola de nieve", en el que los participantes del estudio indican nuevos participantes, creando una red social que se expande a partir de las conexiones de los entrevistados[47]. Ese método presenta la ventaja de posibilitar el acceso a grupos de difícil alcanze, como especialistas. Por tratarse todavía de un muestreo no-probabilístico, no garantiza la representatividad de la población estudiada y es más sensible a siesgos de selección, lo que constituye una limitación metodológica de esta pesquisa. Los participantes iniciales se definieron a partir de las redes sociales del equipo del proyecto y de indicaciones de ISOC Brasil, siendo favorecidas personas con expertise o participación previa en la discusión pública sobre los temas de cifrado, privacidad y seguridad de la información. En total, se enviaron 76 invitaciones a posibles entrevistados.

Se realizaron 45 entrevistas: una de ellas fue exclusa del análisis porque las respuestas fueron insuficientes y otra porque se constató posteriormente que el entrevistado no poseía vínculo con el sector analizado. De las 43 entrevistas consideradas válidas, 13 fueron conducidas con representantes del sector privado y 10 con cada uno de los demás sectores (comunidad académica, sociedad civil organizada y sector público). Hubo paridad de género en todos los sectores, excepto el privado, con 8 entrevistados del género masculino y 5 del femenino.

Cuanto al área de formación, hubo una predominancia del área jurídica (27 entrevistas), seguido por el campo computacional (8, incluyendo Ciencia de la Computación, Redes e Ingeniería de la Computación), Ciencias Sociales (5), Comunicación (4), Administración Pública y Políticas Públicas (3), Ciencia Política y Relaciones Internacionales (2), Economía (1), Historia (1), Administración(1), Artes Visuales (1) y área interdisciplinar (3). Todavía, 14 de los entrevistados poseían múltiples formaciones, sea por haber hecho múltiples graduaciones o por haber hecho la graduación y post-graduación en áreas distintas.

Cuanto a la actuación profesional, las trayectorias son bastante heterogéneas. Entrevistamos gestores de relaciones gubernamentales de grandes plataformas digitales, investigadores de ONGs de tecnología y derechos humanos, profesores universitarios

47 VINUTO, J. A amostragem em Bola de Neve na pesquisa qualitativa: um debate em aberto. **Temáticas** (UNICAMP), v. 44, p. 201-218, 2014.

dedicados a pesquisar temas conexos, servidores de agencias reguladoras relevantes para el campo tecnológico, investigadores de maestria y/o doctorado direccionados hacia los temas de internet y sociedad, abogados especializados en derecho digital, operadores de la justicia criminal en los niveles federal y estadual, asesores parlamentares federales, activistas de derechos digitales y software libre, analistas de ciberseguridad de entes públicos y privados, consultores privados de seguridad de la información, entre otros vínculos de los entrevistados.

3.2. Realización de las entrevistas

El guion de las entrevistas contenía preguntas referentes a los siguientes temas: trayectoria profesional y académica; importancia atribuida a la privacidad y al cifrado; percepción sobre la relación entre privacidad y seguridad; satisfacción con el ambiente regulatorio nacional; opinión sobre acceso excepcional y riesgos percibidos; opinión sobre el debate público relativo a la privacidad en Brasil; opinión sobre medios alternativos de acceso a contenido cifrado que no involucraran interferir en el cifrado; y opinión sobre la legitimidad de los bloqueos de WhatsApp en Brasil. Para entrevistados con formación jurídica, también se preguntó sobre su entendimiento sobre la licitud de bloqueos judiciales de aplicación con base en el Marco Civil de internet. Para entrevistados del sector público, su cuestionó sobre su evaluación sobre la importancia atribuida a la seguridad en la información en el contexto de la digitalización gubernamental. Se puede consultar su íntegra en el Apéndice 1.

Las entrevistas tuvieron carácter semiestructurado, es decir, el guion funcionó como un conjunto de directrices previamente fijadas, no como un protocolo a ser seguido estrictamente en cada interlocución concreta, y conducidas de modo similar a conversaciones informales[48]. Esa opción metodológica intentó favorecer el establecimiento de una relación de confianza y seguridad con los entrevistados, de modo a dejarlos más a gusto para falar de forma más libre y sincera - requisito necesario a la realización de entrevistas que produzcan mayor riqueza de datos[49] -, sobre todo a causa del carácter polémico y sensible de algunos de los temas tratados. Adicionalmente, esa opción ha posibilitado una exploración más profunda de las perspectivas y saberes específicos de los entrevistados.

Esa opción, sin embargo, contribuyó para que ni todos los entrevistados respondieran a la totalidad del guion uniformemente. Eso ocurrió en parte porque la exploración más profunda de sus respuestas a cuestiones específicas ocupó parte del tiempo de entrevista que sería completado por otras cuestiones, lo que exigió que temas específicos fueran priorizados según el caso concreto. Paralelamente, la anterior heterogeneidad

48 BONI, V.; QUARESMA, S. J. Aprendendo a entrevistar: como fazer entrevistas em Ciências Sociais. **Em Tese - Revista Eletrônica dos Pós-Graduandos em Sociologia Política da UFSC**, Florianópolis, v. 2, n. 1 (3), p. 68-80, en./jul. 2005, p.75.

49 GASKELL, G. Entrevistas individuais e grupais. In: BAUER, M. W.; GASKELL, G. (Org.). **Pesquisa qualitativa com texto, imagem e som**: um manual prático. Petrópolis, RJ: Vozes, 2000, pp. 64-89, p 74.

de trayectorias y saberes también ha favorecido esa variación, pues tales cuestiones relativas a áreas del conocimiento o sectores específicos no necesariamente hacían sentido para todos. Por ejemplo, una cuestión sobre la interpretación de dispositivos específicos del Marco Civil de Internet presuponía algún grado de conocimiento jurídico por el entrevistado, de modo que no haría sentido colocarla en todas las entrevistas.

3.3. Codificación y análisis de los datos

Después de la realización de las entrevistas, se transcribió su contenido y se elaboró una estrategia de manejo para que los datos generados permanecieran en sigilo y en seguridad. Primeramente, se sustituyeron los nombres reales de los entrevistados por nombres ficticios generados por un software generador de nombres y se creó una tabla de conversión. Los archivos fueron cifrados e insertados en una aplicación de nube cifrada. Los investigadores involucrados en esa etapa de análisis bajaron y alocaron los archivos (entrevistas, transcripciones, la tabla de conversión de nombres) en un compartimento cifrado de sus dispositivos locales. La llave para descifrar fue compartida a través de una aplicación de mensajería - igualmente encriptada y con la funcionalidad de auto destrucción del mensaje después de algunos minutos. A fin de excluir permanentemente los archivos originales de los ordenadores personales, se utilizó la herramienta BleachBit - que destruye los rastros digitales de los archivos. Una vez descifrados, se pudo hacer el análisis con el manejo de los materiales anteriormente alocados en el compartimiento codificado. Las transferencias de unidades de análisis entre los investigadores también se realizaron a través de canales codificados.

El contenido de las entrevistas fue entonces sometido, al análisis cualitativo, que consiste en “un conjunto de técnicas de pesquisa para tornar válidas y replicables inferencias de textos (o otro material significativo) a los contextos de su uso”[50]. La codificación y el tratamiento estadístico de los datos cualitativos fueron auxiliados por el software Atlas.ti 7.0, que ofrece una miríada de herramientas destinadas a amparar investigadores en el análisis cualitativo[51]. A pesar de sus beneficios, es importante destacar que el programa no conduce hacia el análisis solo y es necesario que los investigadores produzcan las conclusiones a partir de sus aportes conceptuales y epistemológicos.

El análisis cualitativo sistemático tuvo carácter inductivo, es decir, la construcción de los códigos y categorías de análisis se realizó con base en lo que se aprehendió de los propios datos a partir de una exploración inicial, y no en un conjunto predefinido de criterios. Asumiendo un enfoque interpretativo, buscamos reconstruir los sentidos dados por los entrevistados a los temas discutidos, lo que posibilita tanto una aprehensión general de sus creencias, visiones de mundo y argumentos cuanto a generación de nuevas hipótesis

50 KRIPPENDORFF, K. **Content Analysis**: an introduction to its methodology. Thousand Oaks, Calif.: Sage Publications, 2004, p.18.

51 SILVA JUNIOR, L. A.; LEAO, M. B. C. O software Atlas.ti como recurso para a análise de conteúdo: analisando a robótica no Ensino de Ciências em teses brasileiras. **Ciênc. educ.** (Bauru), Bauru , v. 24, n. 3, p. 715-728, sept. 2018.

sobre el conjunto de fenómenos discutido en la entrevista a partir de las teorías nativas de esos profesionales[52].

A fin de restringir el ámbito del análisis, se seleccionaron cuatro temas generales explorados en diferentes segmentos de las entrevistas: i) implementación de acceso excepcional en sistemas criptográficos para acceso datos cifrados para fines de persecución penal; ii) conocimientos y riesgos sobre potenciales alternativas para acceso de las autoridades al contenido descifrado sin interferencia directa en el cifrado; iii) el ambiente regulatorio nacional referente a la cifrado; iv) los bloqueos de WhatsApp en Brasil y su relación con el Marco Civil de Internet.

Para codificación y análisis de cada uno de esos temas, se siguió el procedimiento a continuación: distribución de las entrevistas entre los investigadores responsables por la parte empírica de la pesquisa para exploración inicial y codificación abierta del segmento, seguida por una revisión conjunta de la totalidad del universo codificado y consolidación de los códigos. Con base en eso, se buscó establecer relaciones de significado entre los códigos y, a partir de ellas, reconstruir narrativamente los principales argumentos y encuadramientos dados por los entrevistados a los temas tratados. En razón de la replicación cuádrupla de ese procedimiento, se produjeron cuatro esquemas de codificación distintos e independientes, que se pueden consultar en el Apéndice 2.

3.4. Limitaciones de la metodología adoptada

En razón del carácter no-probabilístico de la metodología de selección adoptada, como también del carácter semiestructurado de las entrevistas y de las variaciones en la aplicación del guion, los resultados abajo presentados no deben ser interpretados como representativos de las opiniones o actitudes de cualquier segmento poblacional.

Lo que ellos constituyen es un panorama empíricamente fundamentado de creencias, argumentos y racionalidades que cruzan el debate público sobre *Going Dark* y *Crypto Wars* en Brasil, según se pudo extraer a la luz de 43 entrevistas con profesionales que participaron de la construcción de ese debate.

4. Resultados

Esta sección presenta los resultados del análisis de contenido. Se presentan los resultados en la forma de reconstrucciones narrativas sobre las categorías de enunciados más frecuentes, a fin de evidenciar las conexiones lógicas que permean sus racionalidades.

52 ROSENTHAL, G. **Pesquisa social interpretativa**: uma introdução. Porto Alegre: Edipucrs, 2014.

Todos los nombres utilizados son ficticios y fueron determinados aleatoriamente a partir de un software generador de nombres. Los énfasis en las citaciones son obra de los investigadores del estudio.

4.1. Sobre la inserción de mecanismos de acceso excepcional en la cifrado

Las cuestiones sobre mecanismos de acceso excepcional fueron respondidas por todos los entrevistados.

4.1.1. El discurso favorable al acceso excepcional

El apoyo al acceso excepcional se fundamenta en el entendimiento de que el acceso a las comunicaciones privadas es **necesario para la seguridad pública (argumento usado 4x)**, valor que se debería priorizar cuando en conflicto con otros derechos, como privacidad y libertad de expresión. Según ese raciocinio, los daños causados por ciertos crímenes - por ejemplo, secuestros, tráfico de drogas, abuso infantil, terrorismo – son tan graves que justifican la relativización de esos derechos en nombre del interés colectivo.

Además, **ciudadanos y empresas tienen la obligación de obedecer a la justicia (7x)**, lo que implica en el deber de cumplir órdenes judiciales de entrega de datos para investigaciones criminales, aunque eso exija debilitar la cifrado. Eso porque el acceso excepcional ya sería legalmente previsto por ser **equivalente a una interceptación telefónica (3x).** En ese caso, se comprende que la prerrogativa de acceso estatal a comunicaciones privadas en los casos previstos por la Ley de las Interceptaciones Telefónicas se amplía a las plataformas digitales. En las palabras del entrevistado Afonso:

> Ya he estado del otro lado. Ya he estado del lado que tiene que encarcelar al bandido. Y te da trabajo cuando estás con los datos todos cifrados [...] Mecanismo excepcional es una palabra también que funciona bien. Es un acceso excepcional, es el acceso del interceptor telefónico. La **policía no intercepta a todo el mundo à sin discriminación, hay una regla. Para mí, esa regla puede ser la misma regla para interceptar el Whatsapp**.
>
> Afonso tiene formación en el área computacional, con foco en seguridad de la información, y tiene amplia experiencia en docencia, consultoría privada en redes y gestión de proyectos.

En ese punto, hay quien considere, incluso, que **el acceso excepcional sería un medio investigativo tan o menos pesado que los empleados actualmente (2x)**. El raciocinio es el siguiente: una vez que es necesario acceder a tales comunicaciones para investigaciones

de alguna forma, el acceso excepcional permitiría acceder al canal objetivado de forma precisa. Eso causaría daños menores que los de una busca y embargo, por ejemplo, que además de suprimir la inviolabilidad del domicilio, posibilita la busca en todo dispositivo y todas las informaciones en él contenidas. Esa es la visión de la entrevistada Thais, por ejemplo:

> "Gente", sería mucho mejor si uno trabajara con determinada aplicación que uno dijera "yo quiero saber solo los mensajes de WhatsApp". Y solo WhatsApp, no quiero ver sus fotos, su lista telefónica, lo que conversas con tu mujer, ¿me entiendes? [...] Sería mucho más práctico. Entonces acaba que **por falta de determinadas aplicaciones para hacer y tener acceso a esos mensajes, uno utiliza a veces de mecanismos más invasivos de lo que necesitábamos muchas veces**."
>
> Thais tem formação jurídica e atua no sistema de justiça criminal, com foco em crimes cibernéticos

Cuanto al potencial de abuso por la autoridad, esos riesgos serían mitigados por la existencia de **controles institucionales robustos (11x)**. Tales controles incluyen la existencia de orden judicial específica y fundamentada, con determinación de la finalidad y de los individuos específicos a ser afectados. Con frecuencia se resalta que eso debería ser un recurso accionado **solo en casos de crímenes graves (7x)**, como los mencionados, y c**uando ya se agotaron otras posibilidades de investigación (3x)**. Junto a eso, por veces aparece la percepción de que es **necesario confiar en las instituciones (2x)**. El entrevistado Julian lo resume bien:

> Ahora, yo tengo que confiar en la justicia. Yo, como abogado... Existiendo una ley que diga cuándo, cómo, en qué condiciones y que solo en esas condiciones eso puede pasar y hay una autoridad judicial investida por el Estado para tomar esa decisión, **si no confío en eso, no puedo confiar en nada en la justicia**. Sería una confianza selectiva: "No, yo confío en la justicia, pero eso no". ¿Por qué? Hay tribunal, hay dirección general de justicia, hay CNJ, nosotros tenemos que confiar. [...] No existiendo otro recurso y delante de una eventual gravedad del crimen, con ley propia diciendo cómo eso va a pasar, con decisión judicial específica y fundamentada, ahí yo pienso que sí, yo pienso que nosotros tendremos de enfrentar circunstancias [en las] que la paz social es más importante que la paz criminosa.
>
> Julian tiene formación jurídica, amplia experiencia en el sector público con regulación de tecnología y trabaja en el sector de relaciones institucionales de una gran empresa

Defender que el Estado tenga acceso a contenidos cifrados para fines de investigación aparece, todavía, como **una forma de reafirmar la autoridad pública (1x).** En esa línea, la defensa del acceso excepcional reiteraría simbólicamente que la competencia investigativa y la autoridad general del Estado están arriba de intereses y decisiones de empresas privadas, las cuales podrían encontrarse en la posición de desafiarlas en virtud de su poder global. Para Natália, la defensa del acceso excepcional se conecta a esa disputa simbólica.

> Las empresas necesitan decidir colaborar con nosotros, con la misma sociedad. Porque la empresa hace su modelo de negocios y ellos quieren ganar dinero, entonces **si no existe una presión del poder público para que haya esa colaboración, ¿por qué van a gastar dinero montando todo un sector de una empresa para dar soporte para las autoridades públicas?** Entonces uno piensa, uau, hoy Google, Facebook, tienen oficinas y sectores totalmente montados para dar soporte al *law enforcement*, a la investigación de autoridades públicas. ¿Por qué lo harían si no hubiera una presión del sector público en ese sentido? Entonces es necesaria esa presión.
>
> Natalia tiene formación jurídica y actúa en el sistema de justicia criminal, con foco en crímenes cibernéticos

4.1.2. El discurso contrario al acceso excepcional

El rechazo al acceso excepcional tiene como base la percepción de que la medida **contraría principios básicos y buenas prácticas de seguridad de la información (20x)**. Eso porque el aumento en la complejidad de un sistema necesariamente reduce su seguridad, sobre todo mediante la introducción intencional de una vulnerabilidad a ser utilizada regularmente. Así, el acceso excepcional fue descripto como una medida que "debilita la tecnología como un todo" y "estaría rompiendo la confiabilidad de la cifrado por esencia".

Conectados a tal preocupación estuvieron los dos principales riesgos apuntados. El primer fue de que **el mecanismo fuera explorado por terceros maliciosos (18x)**, a ejemplo de criminosos cibernéticos y gobiernos extranjeros, que podrían hacer uso de la vulnerabilidad para fines ilícitos. De ese modo, la propia **seguridad del Estado sería debilitada (4x)**, una vez que la confidencialidad de las comunicaciones de las propias autoridades depende de plataformas cifradas. Es esta la perspectiva del entrevistado Alvin:

> Supongamos por un momento, esa es una hipótesis muy dura, en la cual no creo- en términos personales no la creo-, pero supongamos que hay buenos actores y malos actores. Supongamos que vivo en un país de buenos actores y que hay una buena política, un buen MP,

> buenas autoridades, todos son moralmente buenos, ¿supongamos eso, bien, ok? La pregunta es: ¿esas buenas personas deben poder acceder con acceso excepcional para poder investigar situaciones ilegales? Bueno, yo podría pensar: sí, ¡porque son buenos! Yo soy bueno, ellos son buenos, queremos proteger a los buenos. El problema es que esa lógica no existe. No creo en esa lógica. No son solo buenos, hay de todo. Pero siguiendo esa lógica, el problema es que en el mundo ni todos son buenos, hay otros países, hay otras organizaciones, hay hackers, hay mafias, hay otros estados, ¿verdad? **Entonces cuando se crea ese acceso excepcional para los "buenos", para esa gente pura que quiere protegerme y cuidarme, cuando se crea ese acceso excepcional para ellos, también se abre una vulnerabilidad para otros**. Entonces, en realidad, está creando una vulnerabilidad que puede ser explorada por otros gobiernos, otras organizaciones, por otras empresas, otros hackers, …..
>
> Alvin es economista, tiene amplia experiencia en los sectores público y privado y actúa en el sector de relaciones institucionales de una gran plataforma

El segundo principal riesgo fue de que el acceso excepcional fuera blanco de **abuso por las propias autoridades (18x)**, que podrían instrumentalizarlo para vigilancia y persecución política de opositores o recorrer al mecanismo de forma amplia y generalizada. A ese respeto, se destacó una preocupación con una **posible banalización de las roturas de sigilo (3x).** La entrevistada Vitória resume la preocupación:

> Como yo lo decía antes, las roturas tienen contenido exploratorio. Y más que eso , aún antes de tener contenido exploratorio, en regla son usadas como primer recurso de investigación. [...] Las interceptaciones telefónicas, telemáticas... Está escrito en la Ley 9296 que deberían ser usadas como último recurso de investigación, cuando todo el resto falla y se muestra insuficiente. Pero uno percibe una banalización, y una tendencia de los jueces... De las autoridades policiales para pedir , del MP también, y de los jueces para deferir sin criterios y sin una demostración efectiva de que algo habría que ser hecho antes, para que se demuestre una necesidad intransponible de romperse ese tipo de dato. **Entonces yo entiendo que si uno lleva adelante ese discurso también en relación al cifrado, este será roto como regla y de forma extremamente amplia**.
>
> Vitória tiene formación jurídica y amplia experiencia abogando en la intersección entre proceso penal y nuevas tecnologías

Otro argumento frecuente fue el de que **hay o debe haber medios alternativos de investigación (19x)**, entre los cuales se comentaron: análisis de metadatos, busca y

aprensión de dispositivos, recuperación de los datos almacenados en *backups* en la nube e infiltración policial. A ese raciocinio se alía el argumento de que **necesidad y eficacia de la medida no fueron suficientemente demostradas (6x)**, a la vista de la ausencia de datos conclusivos referentes al número de investigaciones que de hecho no alcanzan éxito debido al cifrado. Además, hay **posibilidad de criminales abandonar plataformas en la que se debilitó el cifrado (8x)**, lo que tornaría la eficacia del acceso excepcional nula. Los entrevistados Gilson y Maiara sintetizan esos dos últimos argumentos:

> Tengo mucha curiosidad en saber también los números de situaciones en las que la policía no consiguió resolver la causa del cifrado, cuál es el porcentaje. Y pienso que ese es un dato muy oculto, que para mí es siempre un hueco. Siempre que voy a dar una clase "me quedo así": **tío, uno no sabe si el cifrado, hoy, es un problema**. Porque, así, tal vez todo lo que digo cambiaría si la gente percibiera que, no sé, un 95% de los crímenes de Brasil no se solucionan a causa del cifrado, pues este los está afectando. Bueno, tal vez uno cambiara de idea. Pero uno no sabe si es el 0,000009% de los crímenes, entonces se pone difícil saber de esos dos extremos, dónde uno está."
>
> Gilson es jurista, experimentado en el sector público y en docencia, su producción académica se direcciona hacia cuestiones involucrando internet y derechos fundamentales

> Tengo esa percepción de que es muy complicado porque en la medida en que algunas empresas pasan a dar ese acceso, **uno sabe que la criminalidad migra**. Igual uno va a cambiar mudar para el Signal, ellos migran. Grandes organizaciones criminales hoy contratan técnicos y ellos tienen condición de hacer su propia aplicación de mensaje que no va a dar acceso al *law enforcement*, que no va a dar acceso, y ahí estarás haciendo todo ese movimiento, disminuyendo – y yo tengo esa percepción, que va a estar disminuyendo, sí– la seguridad de las informaciones de las personas , y las nuestras.
>
> Maiara es periodista, experimentada en producción audiovisual y trabaja con educación de grupos activistas, con foco en seguridad digital

Bajo ese punto de vista, el acceso excepcional sería desproporcional en la medida en que **afecta a los derechos de todos los usuarios (26x)** e impacta su seguridad, privacidad y libertad de expresión en nombre de la resolución de algunos crímenes. Eso atingiría sobre todo periodistas, activistas, minorías sociales y opositores gubernamentales, los cuales estarían más sujetos a daños si sus comunicaciones privadas fueran violadas. En ese sentido, se notó que la propia posibilidad del gobierno de valerse indebidamente del acceso excepcional ya atingiría derechos en virtud del efecto inhibitorio que la conciencia

de estar siendo vigilado provoca sobre los individuos, lo que podría llevarlos , por ejemplo, a refrenarse de expresar divergencias políticas por temer el monitoreo estatal.

Todavía en ese prisma, se observó que el acceso excepcional **impacta negativamente la confianza en el ecosistema digital (13x)**, lo que es necesario para que los ciudadanos se sientan aptos a hacer uso de los bienes y servicios en un contexto de digitalización. En esa línea, los **costos operacionales y reputacionales impuestos a los proveedores (11x)** fueron citados como causadores de repercusiones económicas negativas, pues la complexidad de desarrollarse y mantener un mecanismo de esa naturaleza sería elevada y plataformas que se valen del uso del cifrado como un diferencial competitivo asociado a la mayor seguridad, como WhatsApp, sufrirían un enorme daño a la marca y podrían tener sus modelos de negocios inviabilizados.

4.2. Sobre alternativas al acceso excepcional

Cuanto al conocimiento de métodos y técnicas alternativos capaces de proveer a las autoridades acceso al contenido de datos protegidos por cifrado para fines de investigaciones criminales, 33 de los 43 entrevistados respondieron a esa cuestión. De los 33 respondientes, **7 afirmaron no acordarse o desconocer alguna alternativa**. De ese modo, fueron 26 respondientes que hablaron sobre alternativas y métodos o técnicas.

Una de las principales alternativas citadas para el acceso a los datos fue la **aprehensión de los dispositivos específicos relevantes para el caso (6x)**. Una vez realizada la aprehensión, las autoridades podrían acceder a su contenido. Si el contenido está protegido por algún recurso de seguridad, como cifrado de disco, las autoridades podrían proseguir de dos formas: I) obligar, a través de orden judicial, algún usuario que conozca la contraseña o llave de acceso a proveerla; o ii) lanzar mano de herramientas que exploran vulnerabilidades en la tecnología para burlar los mecanismos convencionales de autenticación.

Esa segunda hipótesis está conceptualmente próxima de todo un abanico de alternativas objeto de frecuente citación y agrupadas bajo las rubricas de ***government hacking* o *lawful hacking* (19x)**: el uso de técnicas y herramientas destinadas a comprometer la seguridad de dispositivos o softwares utilizados por las personas bajo investigación, a fin de posibilitar la obtención de los os datos necesarios a la producción de las pruebas. En ese universo, métodos específicos citados incluyeron:

- **Busca exhaustiva de llave (3x):** La utilización de métodos computacionales para romper la seguridad de un sistema criptográfico, a fin de descifrar texto sin que se tenga acceso autorizado a la llave del descifrado. Ejemplos incluyen ataques de fuerza-bruta, en los que un elevado número de llaves o contraseñas posibles es recorrido en alta velocidad, o de diccionario, en el que se recorre una lista predefinida de posibles llaves o contraseñas Esa solución sería adecuada para casos en los que el cifrado utilizada no es computacionalmente segura

o cuando el sistema no posee protecciones contra la ejecución de un número muy elevado de intentos.

- **Ingeniería social (3x)**: la autoridad policial encubriría su identidad en una interacción con la persona investigada, a fin de inducirla a cometer un ato que comprometiera la confidencialidad de sus informaciones, como el envío de credenciales de acceso a cuentas o a la inoculación de software malicioso en su dispositivo.

- **Spyware (7x):** la introducción oculta de código malicioso en el sistema atacado para la exploración de vulnerabilidades no-solucionadas por sus desarrolladores, lo que favorecería la recolección remota de los datos necesarios a la investigación. Dependiendo de la herramienta utilizada, sería posible activar el micrófono, la cámara y/o la geolocalización del dispositivo, como también registrar mensajes digitados y/o enviados, sites y aplicaciones utilizados.

Un segundo conjunto de soluciones mencionadas involucraría algún grado de cooperación con las proveedoras de los canales de comunicación. En ese ámbito, se mencionó la técnica de **escaneo del cliente (2x)** (*client-side scanning)*, un mecanismo en el que el software del dispositivo el canal comunicativo testaría el contenido de cada mensaje enviado contra una base de datos predefinidos de contenidos dañosos, que estarían señalados con identificadores únicos. Si una ocurrencia de aquel contenido fuera encontrada en la base, se desencadenaría alguna acción: el envío sería impedido o las autoridades serían alertadas.

Soluciones de llave o usuario fantasma (2x) siguen el mismo espíritu: se demanda que la plataforma implemente un mecanismo para introducir una tercera punta en la conversación sin que las partes comunicándose lo sepan. Una aplicación podría transformar la conversación entre dos usuarios en un grupo del cual la autoridad formaría parte sin que la interfaz de la conversación fuera modificada o que los dos usuarios recibieran cualquier notificación. Paula ejemplifica el funcionamiento de la práctica y junto presenta un punto de discusión.

> Otro método que vimos fue *ghost key*, que es muy defendido en el Reino Unido, que es básicamente cambiar la interfaz para que el usuario no perciba que tiene un agente con él en una conversación, siguiendo su conversación, entonces, en lugar de aparecer tres personas en la conversación, aparecen dos. **Pero hay una gran discusión si eso no es una forma de acceso excepcional más, si tú implementas una vulnerabilidad que se puede considerar acceso excepcional de toda forma.**
>
> Paula, formación jurídica y en área interdisciplinar. Investigadora en el área de privacidad y vigilancia. Experiencia en la sociedad civil y académica.

Otra alternativa fue el **análisis de metadatos (5x)** en un contexto en el que estos no están protegidos con cifrado. De ese modo, sería posible aprehender informaciones sobre el horario de comunicaciones, localización, frecuencia de comunicaciones, etc. El entrevistado Eduardo defiende que la práctica sea, también, acompañada de una preocupación con la privacidad.

> [...] yo no defiendo que haya una colaboración extensiva sobre metadatos porque eso heriría también la privacidad, pero pienso que de otra manera, siguiendo el principio de minimización de recolección de datos, de colaboración puntual, pienso que es posible pensar en formas. Pienso que ese es un debate en construcción en el que ud. preserve lo que se está conversando, lo que está es el mérito, el contenido de la conversación, pero sin proveer a las autoridades judiciales algún tipo mínimo de información de contexto o usando metadatos para expresión técnica. Pero aquí, otra vez, pienso que es un debate en construcción, difícil. Hay otras aplicaciones de mensajería, el Signal por ejemplo, que tiene cifrado, es eso, metadatos se pueden cifrar. Entonces el objeto del cifrado puede ser el contenido sobre que se está conversando, pero el cifrado puede también abarcar algunos metadatos. Y ahí se ud. quiere acceso a los metadatos que están cifrados, también es vulneración de la cifrado.
>
> Eduardo, formación jurídica, amplia experiencia en el sector público, trabaja con relaciones gubernamentales en una gran empresa de tecnología

También se mencionó el **acceso a datos en backups mantenidos por terceros (3x)**. A ese respeto, se destacó la existencia de backups de contenidos de conversaciones que tienen niveles inferiores de protección o son almacenados de forma enteramente descifrada, los cuales ya serían utilizados por las autoridades para contornar el cifrado. En su entrevista, Thais describió cómo se viene utilizando la práctica.

> Y, en verdad, hoy día, con la nube, uno ya lo hace, ¿me entiendes? [...] Cuando uno hace al alejamiento [del sigilo] de la nube, ella acaba por ser así, vamos a decir, como un *backdoor*, es casi no, es un *backdoor*. Porque cuando pide el alejamiento [del sigilo] de la nube porque ud, justamente, ud no tiene acceso a través del cifrado. Pero es así, no son todos los que tienen la nube, hay toda aquella de que ud. haga el backup. Hay nubes de determinadas aplicaciones que son más accesibles, siempre lo han sido. Entonces no es todo el mundo que la utiliza, pero acaba que cuando uno tiene una rotura de esa viene todo de la persona, ¿entendió?
>
> Thais. Formación jurídica, actúa en el sistema de justicia criminal, con foco en crímenes cibernéticos.

Em la misma línea, **el monitoreo de las redes sociales (1x)** fue mencionado como medida que permitiría aprehender informaciones relevantes a la investigación, como viajes realizados, relaciones personales, bienes personales etc

4.2.1. Los riesgos de las alternativas

Junto a la pregunta sobre los métodos alternativos de obtención de datos para investigación que no impliquen en rotura de cifrado, los entrevistados fueron cuestionados, también, sobre los riesgos atribuidos a las prácticas citadas.

Una percepción recurrentemente manifestada fue la de que la mayoría de las alternativas antes mencionadas implica en **riesgos de abuso por la autoridad pública (9x)**, por veces conectados a la posibilidad de **violación excesiva de la privacidad (6x)**. Esa preocupación estuvo asociada sobre todo a las prácticas de *lawful hacking* y aprehensión del dispositivo. En ese caso, el acceso investigativo a la totalidad del dispositivo de la persona investigada podría resultar en la recolección y análisis de datos sobre una serie de actividades e interacciones referentes a su intimidad e irrelevantes para la apuración de los hechos investigados.

Otra preocupación de esa naturaleza fue la posible **violación del debido proceso legal (2x)**, por la posibilidad de busca de pruebas en el medio digital - abundante en información- como un atajo investigativo, aunque los demás medios de producción de prueba no se hayan agotado. Bajo la misma óptica, se expresó preocupación con la **vulneración de terceros no involucrados en la investigación (x1)** y que puedan tener informaciones y comunicaciones personales alocadas en el dispositivo.

En el ámbito de las prácticas que se basan en algún grado de cooperación directa con la plataforma, como escaneo del cliente y soluciones de llave fantasma o usuario fantasma, una percepción manifestada fue la de que tales iniciativas presentarían **riesgos similares a los del acceso excepcional vía backdoor (4x)**, en las palabras de Jéssica:

> Para el derecho de las personas, sí, en una visión más ética, yo pienso que es antiético que ud tenga un usuario fantasma sin que la persona lo haya consentido. Yo pienso que eso es éticamente equivocado. Entonces yo veo que eso puede ser utilizado también para, una vez más, violar otros derechos. ¿Entonces como yo voy a saber si esos usuarios fantasma van a ser colocados en grupos? ¿Los van a utilizar solo para hacer investigaciones criminales, o para (de repente) empezar a intentar verificar qué tipos de debates se están haciendo para bloquear la libertad de expresión? No se sabe. Pienso que caemos en el mismo problema del acceso excepcional, y esas otras cuestiones.
>
> Jéssica, formación en ingeniería, experiencia amplia en organizaciones de gobernanza de la internet.

A ese respeto, dos puntos merecen destaque. En primer lugar, se constató incertidumbre sobre tales soluciones efectivamente no interferir en el cifrado, especialmente en el contexto de las soluciones de llave -fantasma, que implican en interferencia en el mecanismo de gestión de llave, aunque puedan no alterar el proceso de codificación. En segundo lugar, hay la percepción de que aunque tales mecanismos mantengan el cifrado en el sentido estricto, ellos nulifican su propósito: de ese modo, los riesgos de abuso, el efecto inhibitorio y los daños a la confianza en el ecosistema digital estarían presentes de la misma forma. Alvin trata ese problema en su habla:

> Obviamente *ghosting* es lo mismo [que acceso excepcional] [...]. **Un principio fundamental del cifrado es que solo las personas que están participando de esa conversación acceden al contenido.** Cuando hay una tercera persona sin que ud sepa que esta persona está, obviamente hay una violación de la privacidad y pone en cuestión lo que hablábamos antes.
>
> Alvin, economista, ampla experiencia en los sectores público y privado. Actúa en el sector de políticas públicas de una gran empresa.

Por fin, hubo una preocupación general con la posibilidad de **escape de datos en poder de las autoridades públicas (2x)** - dada la falta de confianza en los sistemas de seguridad de la información empeñados por el gobierno con los sucesivos casos de enormes escapes de datos de los ciudadanos brasileños. Hay una preocupación, por lo tanto, con los parámetros de seguridad en los protocolos de archivamento de material digital por las autoridades.

4.3. Sobre el ambiente regulatorio nacional sobre cifrado

Las preguntas sobre ambiente regulatorio fueron respondidas por 42 entrevistados. **5 respondientes afirmaron desconocer el ambiente regulatorio nacional relativo al tema.**

Entrevistados manifestaron el entendimiento de que el **cifrado tiene su importancia reconocida y su uso encorajado (9x),** en una visión recurrentemente positiva del ambiente regulatorio brasileño. Ese incentivo sería resultado de normas con el Marco Civil de Internet, cuyo decreto regulador incentiva expresamente el uso de encriptación para garantía de la seguridad los dados (art. 13º, inciso IV) y la LGPD, que compele a los agentes de tratamiento la adopción de medidas técnicas de seguridad para la protección de los datos contra incidentes (arts. 6º, incisos VII y VIII, 13º, 44º, 46º y 49º). Como argumentado por Carla:

> Lo que la gente tiene de derechos fundamentales y de derechos en general ya sirve para uno basar y proteger el uso del cifrado. [...] yo pienso que, como una persona que investiga ese tema y ve la jurisprudencia y la doctrina caminar hacia ese reconocimiento, **yo creo que lo que uno tiene ya posibilita una legalidad, un ambiente que favorece y entiende la importancia de las aplicaciones cifradas.**
>
> Carla, formación jurídica, actúa como investigadora de las relaciones entre derecho y nuevas tecnologías.

Esa percepción se aliaba a la de que los **últimos años fueron marcados por avances significativos en el debate público sobre el tema (7x)**, lo que fue, por veces, ejemplificado por la referencia a los votos de los ministros del Supremo Tribunal Federal que relataron las acciones relacionadas a los bloqueos de WhatsApp en Brasil. También se mencionó como ejemplo la decisión de la Tercera Sección del Superior Tribunal de Justicia que consideró ilegal la aplicación de multa por no cumplimiento de orden judicial de entrega de datos en razón de imposibilidad técnica de interceptar decurrente de cifrado. Esas decisiones señalarían una evolución en el entendimiento del judiciario sobre el asunto.

En el camino de ese raciocinio, algunos entrevistados evaluaron que **el escenario brasileño es más favorable en relación al cifrado que los de diversos otros países (4x)**, en vista de que no hay prohibición o restricción a su uso y que la interacción entre las normas y los desarrollos jurisprudenciales antes mencionados resultaría en un ambiente bastante favorable a esa tecnología. Carolina trae ese argumento en perspectiva con el contexto internacional.

> Por otro lado, el hecho de que nosotros no tenemos la prohibición, que es algo que muchos países están sufriendo, incluso países democráticos, **son golpes que países democráticos incluso están sufriendo a causa de esa agenda de la seguridad nacional,** países que tienen histórico de terrorismo y por ahí va, en ese sentido pienso que uno todavía está bien.
>
> Carolina, formación interdisciplinar, amplia experiencia con advocacy en cuestiones de tecnología, actúa con seguridad digital para defensores de derechos humanos.

Por otro lado, una impresión común fue que **el debate todavía necesita evolucionar en contenido y alcance (6x)**. Ese avance tendría dos dimensiones: en primer lugar, sería necesario madurar el entendimiento de las autoridades sobre el tema, a fin de garantizar que comprendan la importancia del cifrado y las consecuencias de su debilitación, como también la relación entre su protección y la concretización de los derechos conexos positivados en nuestro modelo. En segundo lugar, sería importante ampliar el alcance de la discusión, a fin de que la sociedad como un todo, y no solo algunos expertos y activistas, comprenda, valorice y defienda el cifrado.

En ese sentido, diversos entrevistados expresaron preocupación con el escenario presente, argumentando que el **cifrado está amenazada (10x)**. Las amenazas citadas incluyen propuestas de alteraciones legislativas que debilitarían la seguridad de los sistemas, como obligaciones de implementar sistemas de custodia de llaves o mecanismos de rastreabilidad de mensajes privados encaminados - a ejemplo el PL 2630. También se destacó que el STF no ha todavía concluido el juicio de las acciones relevantes al tema, lo que elimina la posibilidad de consolidar un entendimiento futuro que comprometa el uso de la cifrado en el país a pesar de los votos iniciales de los relatores de las acciones. En su habla, Paula presenta esas preocupaciones:

> Pero el legislativo es todavía preocupante **porque diversos PLs buscan establecer mecanismos de debilitación de cifrado, sea por acceso excepcional, sea por otros medios.** Entonces pienso que esa pauta podría estar mejor posicionada en Brasil.
>
> En relación a nivel global pienso que la narrativa es bien parecida en muchos países, entonces... Países que se consideran democráticos, ven el cifrado con malos ojos. Esa semana, si no me equivoco fue esa semana, un comisario de RU [Reino Unido] dijo que el cifrado es uno de los mayores obstáculos para el combate a la pedofilia. **Entonces, esas narrativas y esos posicionamientos vienen debilitando la fuerza del cifrado como, digamos, aseguradora de derechos alrededor del mundo también. Entonces, es bastante preocupante** [...].
>
> Paula, formación jurídica y en área interdisciplinar, investigadora en el área de privacidad y vigilancia. Experiencia en la sociedad civil y académica.

Ese raciocinio también se alía a la lectura de que **hay poca o ninguna regulación referente al cifrado en Brasil (12x)**. Esa perspectiva entiende que nuestro modelo legislativo no trata del cifrado, sino de conceptos con un grado más elevado de abstracción, como privacidad y seguridad. Además, el país no dispone de un ente público actuante en el establecimiento de patrones tecnológicos, como el Instituto Nacional de Patrones de Tecnología (NIST) de los Estados Unidos.

> Bueno, yo diría que en relación a la cifrado, **yo diría que uno tiene casi nada de regulación.** Uno tiene algunas directrices que hablan de la importancia de usar, pero pienso que se tiene muy poco de regulación sobre el cifrado. Yo diría que estoy bastante insatisfecha. Lo que en una escala de 0 a 10.. Totalmente insatisfecha sería 0, entonces yo diría que estoy ahí cerca del 1”
>
> Nicole, formación jurídica y en ciencias sociales, amplia experiencia en el sector privado en empresas de tecnología, actualmente trabaja en un bufete

Del entendimiento de que hay poca o ninguna regulación, dos discursos distintos emergieron.

Uno de les ellos demanda más regulación, aseverando que **debe haber una garantía jurídica explícita del derecho al uso de cifrado (9x)**, y sugiere esa innovación normativa como una medicina contra las amenazas a ese recurso. Esa garantía podría venir en la forma de un dispositivo legal o de una jurisprudencia oriunda de un tribunal superior que tornase ilícita la penalización por el empleo de la tecnología. Por ese motivo, cuando preguntado sobre la satisfacción con el ambiente regulatorio sobre cifrado, Marco se declara poco satisfecho.

> [...] Al mismo tiempo en que no tenemos ninguna ley que prohíba cifrado fuerte para las personas, uno no tiene ninguna ley que apruebe el cifrado fuerte para las personas y diga “eso ahí es un derecho suyo”. Entonces pienso que eso me deja insatisfecho, que la cifrado fuerte debe ser un derecho de que ud. quiera comunicarse. Un derecho suyo, un derecho civil suyo.
>
> Marco, científico social y activista, amplia experiencia en el trabajo con difusión de software libre.

Sin embargo, además de esa demanda por una garantía de uso, se argumentó diversas veces que **debería haber una parametrización legal de la cifrado, a fin de proveer mayor seguridad a los usuarios (14x)**. Tal estandarización podría consistir en una obligación de cifrar las informaciones impuesta a ciertas categorías de entes públicos y privados, como autoridades de seguridad pública, instituciones financieras y proveedores de servicios de mensajería. Alternativamente, se podría instituir una autoridad para el establecimiento de patrones, a ejemplo del NIST en los Estados Unidos.

> [...] Yo dejaría más clara la cuestión de su inviolabilidad [del cifrado]. Entonces, en cuáles casos el cifrado es esencial y no puede ser blanco de órdenes judiciales para [inaudible] ese cifrado y en cuáles casos ella es buena, pero no esencial. **Yo diría incluso que el cifrado fuese obligatoria para ciertas aplicaciones de internet.** Entonces, yo sinceramente pienso que una esencialidad de ella, es decir, cuando es obligatoria; y otro punto es, cuando se puede relativizarla.
>
> Nicole, formación jurídica y en Ciencias Sociales, amplia experiencia en el sector privado en empresas de tecnología, actualmente trabaja en un bufete.

El segundo discurso, por otro lado, considera que **no es evidente que regular cifrado sea positivo (6x)** y cuestiona tanto la necesidad de eso como potenciales efectos negativos de propuestas de esa naturaleza. Se argumenta que el desarrollo y el uso del cifrado ya son permitidos en la medida en que no son objeto de restricción o prohibición legal. Nota,

aún, que el cifrado es tanto una técnica como una ciencia, de modo que regulaciones que incidan sobre el desarrollo del campo en cuestión pueden afectar indebidamente la autonomía intelectual y el progreso científico de investigadores de seguridad de la información. Esa preocupación aparece en el habla de Cristiano, por ejemplo:

> Uno no lo tiene, entonces... No sé si quiero un ambiente regulatorio. No lo sé ahora. Así , depende de lo que quiere decir esa pregunta, porque no quiero a nadie regulando cómo puedo o no puedo dejar de usar cifrado, alguien que me diga, como lo había años atrás. [...] **si uno dice este tipo de cosas, que va a decir el tamaño de la llave que puedo usar, los algoritmos que puedo o no utilizar en términos de limitar la fuerza de los algoritmos que puedo utilizar o obligarme a utilizar algún tipo de backdoor o llave maestra... Olvídate. Estoy bien feliz en no tener nada.**
>
> Cristiano, científico de la computación con amplia experiencia en el campo de la seguridad de la información en la academia y en el sector privado.

El principal fundamento del discurso contrario a propuestas regulatorias que tratan expresamente del cifrado es la percepción de que la **neutralidad tecnológica es positiva y se debe preservar (4x)**. Así, el hecho de los instrumentos presentes no tratar expresamente el cifrado sería una virtud, no un defecto. Una vez que no es posible prever los desarrollos tecnológicos de las próximas décadas, cualquier norma que incida sobre tecnologías específicas tiene el potencial de obsolescencia acelerada, aunque aquellas que presentemente podrían parecer positivas, como el establecimiento de un deber de uso de la cifrado.

> **El problema de que ud. regule mucho es que, en la computación como un todo, ella cambia mucho, cambia diariamente.** Si ud. atiende a un patrón mínimo ud. puede estar confortable , pero después de un año, pero se pasó un año, dos, a veces aquel patrón está desactualizado y ud. va a presentar un certificado de que está en conformidad, y hasta puede no ser punido pero el sistema va a ser invadido de la misma manera, ¿verdad?
>
> Sergio, formación en Ciencia de la Computación. Funcionario federal e investigador.

4.4. Sobre los bloqueos de WhatsApp y su relación con el Marco Civil de Internet

La pregunta sobre la evaluación de los bloqueos del WhatsApp fue respondida por 41 de los 43 entrevistados. La pregunta sobre el Marco Civil de Internet autorizar o no tales medidas fue respondida por 23 de ellos .

Una percepción frecuente entre los entrevistados fue de que l**os bloqueos judiciales de WhatsApp en Brasil fueron ilegítimos (17x)**.

Una de las razones para tal evaluación fue de que los bloqueos se fundamentaron en **interpretaciones inadecuadas del Marco Civil de Internet (11x)**, especialmente de su capítulo III, sección II, que trata sobre la protección de registros, datos personales y comunicaciones privadas. Bajo ese punto de vista, esa sección contendría **sanciones aplicables solo a proveedores que violasen las garantías de la privacidad y de la protección de los datos de los usuarios (11x)**. En la ocasión de los bloqueos, ese requisito no estaría presente, pues el no cumplimiento de comando judicial de reparto de datos con las autoridades para fines de persecución penal no correspondería a una violación a tales derechos.

> Totalmente ilegítimos, porque primero fue un caso de interpretación totalmente equivocada del MCI. Existía un dispositivo en los artículos 11 y 12 que traía **sanciones que se deberían aplicar en el contexto en el que el controlador de datos – aunque MCI no use el término controlador de datos, el contexto es ese- [...] esté ya operando y él no garanta los principios de la privacidad**. Y ahí, por el uso incorrecto, podría ser sancionado.
>
> Ian, formación jurídica y en el área computacional, amplia experiencia en el sector público.

Al contrario, cuando ese no cumplimiento resultara de la incapacidad operacional de producir la información solicitada en razón del cifrado, la incapacidad de observar el orden judicial resultaría precisamente del cumplimiento del deber de garantizar la seguridad de los datos. Adicionalmente, en ese caso, la sanción al proveedor sería ilegítima porque **tal obstáculo técnico tornaría el cumplimiento del orden original imposible(6x)**. De ese modo, la obligación de cumplirla sería similar a la obligación de producir una prueba diabólica, además de representar una penalización de la misma herramienta.

La eficacia material de los bloqueos también fue evaluada negativamente por los entrevistados, que los consideraron **ineficaces debido a la posibilidad de contornarlos por medio de redes privadas virtuales (*Virtual Private Networks* - VPNs)**[53] **(4x)**.

Bajo esa óptica, se tejieron críticas a un **desconocimiento de las autoridades judiciales sobre el funcionamiento de la tecnología (8x)**. De ese desconocimiento sobre el cifrado advendría una expectativa, por parte de los decisores, de acceso facilitado a los contenidos de las comunicaciones privadas como un **atajo en las investigaciones criminales (2x)**, como también una frustración cuando de la no concretización de esa expectativa.

53 Recurso tecnológico que establece una conexión de red privada creada sobre una infraestructura de red pública. El uso de VPNs permite que el usuario cifre su tráfico y oculte su identidad y su localización online.

Independientemente de la interpretación del Marco Civil de Internet, con todo, la principal razón para la evaluación negativa de los bloqueos fue el entendimiento de que l**os daños decurrentes de la medida fueron desproporcionales (22x)**. Los derechos de decenas de millones de usuarios de la aplicación fueron atingidos, ocasionando, incluso, **daños económicos a esos usuarios (6x)**. Esa desproporcionalidad tornaría los bloqueos ilegítimos independientemente del contenido del Marco Civil de Internet, una vez que afrontaría directamente preceptos constitucionales como libertad de expresión y libre-iniciativa.

En la misma área, **se cuestionó la competencia del Poder Judiciario brasileño para determinar unilateralmente los bloqueos (2x)** en razón de la medida haber atingido usuarios en otros países de América Latina, representando una extrapolación indebida de la jurisdicción brasileña .

> [...] Y también bajo el punto de vista social, es una decisión muy drástica, porque Whatsapp es uno de los medios de comunicación más utilizado por los brasileños. **Eso tiene consecuencias negativas tanto para las personas que están utilizando esas aplicaciones, para el trabajo, para hablar con sus familiares, como también hasta mismo económicas, porque hay gente que depende de eso para conseguir vender comida, vender...** no sé, cosas que ella tiene allí, los contactos y que dependen de eso para hacer actividades diarias. Entonces ese nivel de bloqueo es tan drástico que tiene efectos bastante negativos para las personas como un todo. Pienso que es una decisión bastante equivocada.
>
> Laura tiene formación jurídica. Experiencia con investigación y activismo involucrando tecnología y sociedad en el tercer sector.

Además del debate sobre el mérito de los episodios, los entrevistados también reflexionaron sobre sus causas concretas, en general atribuyéndolos a una **disputa política entre Facebook y las instituciones del sistema de justicia criminal brasileño(10x)**. Se recordó que la primera orden de reparto de datos cuyo no cumplimiento resultó en el bloqueo precedió la implementación del cifrado de punta-a-punta, siendo su no cumplimiento atribuido a la negligencia de la empresa para con las autoridades nacionales. Tal negligencia habría ocasionado una reacción de reafirmación de la soberanía nacional por medio de la determinación de los bloqueos, de modo a compelir a las empresas a la observancia del escenario nacional.

> Entonces esos bloqueos acabaron ocurriendo por un desprecio de una empresa que viene a trabajar en Brasil, que tiene oficina en Brasil, que es la oficina de marketing de Facebook y que gana dinero en el territorio nacional a partir de los datos recogidos de las personas en territorio nacional y que **no se ha preocupado en tener**

> **un departamento jurídico a la altura para dar el atendimiento a la justicia en Brasil.**
>
> Natália, formación jurídica, actúa en el sistema de justicia criminal, con foco en crímenes cibernéticos.

> Si el cifrado es legal en el país, y no se prohíbe su uso es necesario que se acepte de hecho la incapacidad técnica de entregar ese tipo de contenido. Lo que la justicia brasileña puso en escena en aquella ocasión fue una pulseada con las empresas que no tuvo buenos resultados. No tuvo buenos resultados ni para el caso específico, ni para la cuestión regulatoria más amplia. **Siendo el cifrado legal, no creo que las empresas estén equivocadas en ese caso o resistiendo a un orden judicial. Ellas están preservando la integridad de un sistema que se apoya en el uso de cifrado.**
>
> Tatiana, formación jurídica, amplia actuación en la sociedad civil con defensa de los derechos humanos, investigadora en privacidad y seguridad.

Con menor frecuencia, hubo entrevistados que consideraron que l**os bloqueos fueron legítimos (6x)**.

La primera tesis a ese respeto afirmó que el **art. 11 fundamenta los bloqueos al condicionar el tratamiento de datos a la observancia de la legislación brasileña(3x).** Según ese raciocinio, el no cumplimiento de un orden judicial legítima de reparto de los datos implica en no cumplimiento de la legislación brasileña, una vez que el orden en cuestión se basa en normas que componen el modelo legal nacional.

Para esos entrevistados, el primer bloqueo es especialmente relevante, una vez que la empresa no podía alegar que el uso de cifrado representara un impedimento técnico al cumplimiento del orden. De esa manera, la opción por la inobservancia del orden no representaría solo un desafío político a la autoridad del Poder Judiciario nacional, sino una efectiva violación del orden legal brasileño. De esa forma, constituiría infracción al art. 11 del Marco Civil, lo que atraería la aplicación de las sanciones previstas en su artículo 12, entre ellas, la suspensión y la prohibición de las actividades que involucran los actos previstos en el art. 11.

> Entiendo que sí, que él sí autoriza, porque cuando él dice... [...] 'en cualquier operación de recolección, almacenamiento, guarda y tratamiento de comunicaciones en que por lo menos uno de esos actos ocurra en territorio nacional, se deberá obligatoriamente respectar la legislación brasileña, y los derechos a la privacidad, a la

> protección de los datos personales y al sigilo de las comunicaciones privadas y de los registros'. Entonces uno entiende que **en el art. 11, si todos esos actos - está muy claro aquí -, ellos deben obedecer a la legislación brasileña, cualquier orden judicial que determine el alejamiento del derecho a la privacidad o a la protección... para alejarse de ese derecho de la privacidad o para alejarse el sigilo de comunicaciones, hay que obedecerse la legislación brasileña.** Cuando se dice esto, ya significa que las sanciones por el no cumplimiento del orden judicial [son aplicables]. Eso [el no cumplimiento del orden] ya es el no cumplimiento de la legislación brasileña. Es eso que uno entiende.
>
> Natália tiene formación jurídica y actúa en el sistema de justicia criminal, con foco en crímenes cibernéticos.

Alternativamente, otra tesis entendió que l**os bloqueos podrían ser determinados independientemente del Marco Civil de Internet en virtud del poder general de cautela del juez (3x)**. Mientras garantía de la efectividad procesual, tal figura implica que el magistrado tiene el deber-poder de conceder medidas cautelares atípicas - no previstas en la norma legal – en la ocasión en la que las medidas previstas no sean adecuadas o suficientes al caso concreto. Bajo ese punto de vista, el caso en discusión accionaría tal prerrogativa, sobre todo en razón de medidas anteriores ya haber sido determinadas y la empresa haber recusado a aceptarlas, además de tratarse de crímenes graves - tráfico de drogas.

> Entiendo que el Marco Civil tiene sus sanciones, que no informa quien las va a aplicar y el poder judiciario se ha utilizado de ese artículo para justificar los bloqueos. **Pero mi entendimiento también es que el poder judiciario podría determinar bloqueos sin [el] Marco Civil, porque existe un poder general de cautela del juez para determinar las medidas necesarias para la obtención de material probatorio o eficacia de sus decisiones que se podría evocar sin cualquier necesidad del marco civil.** Tanto es así, que cuando hubo la discusión en el STF, [...] no había necesidad de declaración de inconstitucionalidad de aquellos dispositivos porque con o sin ellos el Poder Judiciario podría haber tomado aquellas medidas. Y la gente va a discutir si eso es legítimo o no a la luz de la constitución, es una otra discusión. Pero realmente en términos de marco normativo, yo pienso que tanto da si el marco civil dice algo o no. Yo pienso que la discusión es realmente de parámetros constitucionales, de control de las decisiones judiciales y no particularmente de la redacción del marco civil.
>
> Silvana tiene formación interdisciplinar en el área jurídica y en el campo de la comunicación y amplia experiencia en el sector público.

5. Análisis y discusión

Esta sección discute el contenido de algunos de los enunciados extraídos de las entrevistas. Cada una de sus subsecciones se direcciona hacia uno de los temas relatados en la sección anterior. Solo no se discuten los enunciados relativos la percepción sobre el ambiente regulatorio, a la vista de que tal ambiente ya se caracterizó objetivamente en las secciones 2.4.2 y 2.4.3 de este estudio.

5.1. Sobre el acceso excepcional

El apoyo a la inserción de mecanismos de acceso excepcional entre nuestros entrevistados se justificó a partir de un raciocinio jurídico-político cuya premisa es la prioridad de la seguridad pública sobre otros derechos amenazados por la medida. Se considera que, si garantizar la seguridad pública exige acceder a comunicaciones privadas, y hay casos previstos en ley para que ese acceso ocurra, es inaceptable que la ley no se cumpla. En esa lógica, los riesgos resultantes del acceso se ven como una carga indeseable, pero necesaria, una especie de "mal menor" si la alternativa es el no cumplimiento de la ley y el impedimento de las investigaciones. De todos modos, los riesgos de abuso podrían ser prevenidos por garantías institucionales, como control judicial y la reserva de ese acceso a casos realmente excepcionales: investigaciones de crímenes graves en los que otros medios investigativos se agotaron. Por fin, sería necesario confiar en las instituciones por principio.

La controversia jurídica evocada por ese punto de vista no se limita a la cuestión del deber de interceptar, sino implica en un debate sobre la existencia o no de un deber de producir una arquitectura tecnológica que permita la interceptación. Como observa Jacqueline Abreu[54], raciocinios como ese "parecen querer extraer de la propia previsión legal en el derecho brasileño de *procedimientos de rotura de sigilo* el deber de que la *habilidad de rotura de sigilo* siempre exista". Para la autora, aunque la existencia de ese deber sea patente en el sector de telecomunicaciones en razón de diversas resoluciones de la Agencia Nacional de Telecomunicaciones que lo prevén expresamente[55], no se puede concluir que se extienda a las empresas de tecnología y proveedoras de aplicaciones de internet, una vez que tales empresas no son concesionarias de servicio público y, por lo tanto, se quedan fuera del escopo de entidades sujetas a las resoluciones antes mencionadas.

El Marco Civil de Internet, a su vez, se restringe a compelir las empresas a la guardia de los metadatos relativos a IP, fecha y hora de acceso. De esta forma, el deber jurídico de

54 ABREU, Jacqueline S.. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Ver. Bras. de Políticas Públicas**, Brasília, v. 7, nº 3, 2017 p. 24-42. p. 32

55 Las normas más relevantes en ese sentido serían las Resoluciones nº 73/1998 (Reglamento de los Servicios de Telecomunicaciones), nº 426/2005 (Reglamento del Servicio Telefónico Fijo Conmutado), nº 477/2007 (Reglamento del Servicio Móvil Personal) y nº 614/2013 (Reglamento del Servicio de Comunicación Multimedios)

tener la habilidad de romper el sigilo de las comunicaciones "no es evidente; necesita fundamentación — y puede muy bien ser que la conclusión sea que no exista"[56]. La cuestión colocada, por lo tanto, es si tal deber debería pasar a existir, lo que evoca consideraciones sobre sus beneficios y daños. En la racionalidad valorativa que basa la defensa del acceso excepcional en el material empírico examinado, el cálculo es nítido: los costos de obstaculización de la persecución penal superan significativamente los riesgos y daños decurrentes de la debilitación cifrada, en especial porque tal punto de vista se basa en una confianza "de principios" en la capacidad efectiva de las instituciones para cohibir abusos de poder.

Cumple notar, con todo, que tal confianza se apoya fundamentalmente en consideraciones referentes a controles institucionales sobre abusos intencionales por la autoridad pública. Sin embargo, no se discute el riesgo de usurpación de la falla de seguridad por terceros maliciosos, como criminosos cibernéticos o gobiernos extranjeros.

Perspectiva divergente es ofrecida por el discurso contrario al acceso excepcional, que presenta dos ejes: la énfasis en los daños decurrentes de la medida en los ámbitos técnico, jurídico-político y económico y el cuestionamiento de su necesidad y de su eficacia. El primer eje asegura que una vez introducida la vulnerabilidad, esta será pasible de uso indebido por criminosos y gobernantes maliciosos. Eso causaría una serie de repercusiones indeseables , entre las cuales se destacan la reducción de la seguridad y de la confianza en el ambiente digital, la violación a los derechos de los usuarios y la imposición de cargas económicas sustanciales a los proveedores.

Las preocupaciones relativas a la seguridad de la información son amparadas por el consenso científico actual en el campo de la seguridad de la información, que atesta la imposibilidad de asegurar solo la exploración lícita y legítima de la referida vulnerabilidad. Todavía, los requisitos de escalabilidad asociados a sistemas de custodia de llave imponen la necesidad de reversión de mejores prácticas de seguridad - a ejemplo del *forward secrecy*, arreglo en el que las llaves de desciframiento se sustituyen inmediatamente después de cada uso, a fin de reducir los daños de su eventual comprometimiento[57]. En ese sentido, la reducción de seguridad resultante de la vulnerabilidad se agravaría porque la reversión correspondiente de esas buenas prácticas implicaría en un aumento de las ganancias de un eventual atacante, lo que ampliaría los incentivos para que la exploración de la falla se concretizara.

Las preocupaciones jurídicas y políticas, a su vez, se alinean a los entendimientos de los relatores de las acciones relativas a los bloqueos de WhatsApp en el Supremo Tribunal Federal, como también al creciente reconocimiento internacional de que el cifrado es necesario para la protección de los derechos a la privacidad y a la libertad de expresión[58].

56 ABREU, Jacqueline S.. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. de Políticas Públicas**, Brasília, v. 7, nº 3, 2017 p. 24-42. p. 34

57 ABELSON, Hal *et al*. Keys under doormats: mandating insecurity by requiring government access to all data and communications. **Journal of Cybersecurity**, v. 1, n. 1, p. 69-79, 2015. p.69.

58 HOBOKEN, J. V.; SCHULZ, W. **Human rights and encryption**. Paris: UNESCO, 2016.

Pero, además de la reflexión abstracta, los apuntes de los entrevistados a ese respecto deben ser entendidos en el contexto del escenario jurídico-político brasileiro, entre ellas, un escepticismo referente a la capacidad de las instituciones de cohibir abusos y una percepción de que habría banalización de las roturas de sigilo en la justicia criminal brasileña.

Cuanto al escepticismo institucional, el examen del ambiente político brasileño ofrece elementos para la apreciación de su pertinencia. En informe conjunto[59] sobre el ambiente político y tecnológico brasileño en el año de 2020, el Centro de Análisis de la Libertad y del Autoritarismo (LAUT) y la Asociación Data Privacy Brasil de Pesquisa (DPBR) identifican trece iniciativas estatales que favorecen el uso de tecnologías de información y comunicación para ampliar indebidamente la vigilancia y el control estatal sobre la población, colocando en riesgo libertades democráticas. Entre las medidas examinadas estaban autorizaciones de roturas de sigilos de datos catastrales sin orden judicial, la construcción de expedientes sobre individuos denominados "antifascistas" y el monitoreo y clasificación de periodistas, parlamentares y formadores de opinión según su posición ideológica. Tales ponderaciones también se amparan por otros levantamientos[60][61], que evidencian una tendencia progresiva a la criminalización y restricción del derecho al protesto en el país desde 2013.

Cuanto a la cuestión específica sobre la existencia de una tendencia judicial a la banalización de las roturas de sigilo, su calibración encuentra obstáculos metodológicos. La Resolución CNJ nº 59/2008 determina que todos los juzgados penales del país provean informes regulares sobre los pedidos de interceptación de comunicaciones y las decisiones de rotura de sigilo. Parte de esos datos se exhiben en formato agregado por medio del Sistema Nacional de Control de Interceptaciones Telefónicas[62]. Sin embargo, el sistema solo exhibe el número de decisiones por tribunal, segmento judicial y tipo de decisión, de modo que no es posible conferir siquiera el porcentual de pedidos deferidos y rechazados. Aunque lo fuera, eso no resolvería la cuestión, que posee una doble dimensión. Bajo el punto de vista descriptivo, sería necesario mapear qué condiciones empíricas han sido interpretadas como suficientes para la contemplación de los requisitos previstos en la Ley 9296. Bajo el punto de vista normativo, sería preciso evaluar si tales interpretaciones son razonables en lo que se refiere a las garantías procesuales. Análisis de contenido jurisprudencial podrán explorar esa brecha en el debate.

59 ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA; CENTRO DE ANÁLISE DA LIBERDADE E DO AUTORITARISMO (LAUT). Retrospectiva - Tecnoautoritarismo 2020. **LAUT,** 2021. Disponible en: https://laut.org.br/wp-content/uploads/2021/01/RETROSPECTIVA-TECNOAUTORITARISMO-2020.pdf. Acceso en: 04/08/2021.

60 ALMEIDA, Frederico de. MONTEIRO, Filipe Jordão; SMIDERLE, Afonso.a criminalização dos protestos do movimento passe livre em são paulo (2013-Es015). **Revista Brasileira de Ciências Sociais** [online]. v. 35, n. 102, 2020.

61 ARTIGO 19. **As restrições ao direito de protesto no Brasil**. 5 anos de junho de 2013: Como os três poderes intensificaram sua articulação e sofisticaram os mecanismos de restrição ao direito de protesto progressivamente. Artigo 19, 2018. Disponible en: https://artigo19.org/5anosde2013/. Acceso el: 04/08/2021.

62 BRASIL. Conselho Nacional de Justiça (CNJ). Sistema Nacional de Controle de Interceptações Telefônicas. **CNJ**, Brasília, 2021. Disponible en: https://www.cnj.jus.br/sistemas/sistema-nacional-de-controle-de-interceptacoes-telefonicas/. Acceso en: 04/08/2021.

Es importante notar, con todo, que hubo un aumento porcentual extremo en el número de decisiones de rotura de sigilo telemático en los últimos cinco años: en todo el año de 2015, se produjeron 1943 decisiones de esa naturaleza, contra 6.898 solo en los seis primeros meses de 2020, representando un aumento porcentual del 255%. Ese crecimiento ya sería notorio en si mismo, pero la ausencia de datos sobre la segunda mitad de 2020 sugiere que sea significativamente mayor. A ese respecto todavía, investigadores de InternetLab[63] observan que los números presentados en el sistema pueden no revelar la grandeza real del volumen de interceptaciones, a la vista de que ya hubo discrepancia histórica entre las informaciones presentes en el sistema y datos oriundos del sector privado: en 2016, el informe de transparencia de la empresa Telefónica (que operaba como Vivo en Brasil) informaba haber recibido 326.811 requerimientos de interceptaciones en Brasil en 2015, un número que ultrapasa tanto el número de cartas expedidas a empresas (95.481) como la suma de teléfonos y teléfonos-VOIP interceptados en aquel año (294.217) según los datos del SNCI.

Para los investigadores:

> Todo eso apunta que los números relativos a interceptaciones en Brasil merecen un estudio propio. Si se revelan altos, pueden sugerir, de un lado, que la protección teórica pretendida por la necesidad de orden judicial y por la previsión de requisitos más rigurosos para realización de ese procedimiento en la Ley de Interceptaciones no se refleja en la práctica. De otro, también puede apuntar hacia deficiencias estructurales en las capacidades investigativas de la policía judiciaria, haciendo con que esta sea fuertemente dependiente de ese medio agresivo de instrucción probatoria. No son pocas las manifestaciones en el sentido de que autoridades de seguridad pública recurren a medidas de interceptación y de rotura de sigilo como *prima ratio*.

Todavía sobre la cultura de interceptaciones en Brasil, el informe de InternetLab recuerda que Brasil ya fue condenado por la Corte Interamericana de Derechos Humanos por conducir interceptaciones telefónicas irregularmente sobre las comunicaciones de trabajadores rurales del Movimiento Sin-Tierra. La irregularidad transcurrió de las interceptaciones haber sido autorizadas por la Policía Militar - que no era competente para hacerlo -, sin notificación al Ministerio Público y fuera del ámbito de una investigación criminal[64] en andamiento. Cumple notar que las autoridades responsables por el ilícito no fueron responsabilizadas.

Las preocupaciones cuanto a los impactos negativos sobre la confianza y la economía

63 ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. **Vigilância sobre as comunicações no Brasil**: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017. p. 44-45

64 Conferir MASI, Carlos Velho. O caso Escher e outros v. Brasil e o sigilo das comunicações telefônicas. **Revista dos Tribunais**, v. 932, Junio de 2013, pp. 309-352

digital, por fin, también demandan testes empíricos. A ese respecto, conviene citar la pesquisa conducida por los investigadores de Law & Economics Consulting Associates y comisionada por Internet Society sobre el tema[65]. El trabajo investigó los costos y beneficios potenciales de la Ley de Alteración de las Telecomunicaciones y de Otras Legislaciones (de Asistencia y Acceso) (LATO) aprobada en Australia en 2018. Esa norma compele proveedores de tecnología de la información a auxiliar a las autoridades en el acceso al contenido de datos cifrados, incluso mediante alteraciones en la arquitectura de sus sistemas. La pesquisa ha articulado entrevistas en profundidad conducidas con los 9 principales proveedores multinacionales actuantes en el país a la aplicación anónima de un cuestionario a otros 79 proveedores.

El estudio concluyó que LATO tendría una serie de impactos negativos potenciales sobre los proveedores y sus clientes. Se destacan , a ese respecto, la ampliación de la incertidumbre en el ambiente de negocios, daños a la imagen de la marca de los proveedores vulnerables a la debilitación de sus servicios y reducción de la confianza en el ambiente digital. Ese último aspecto puede implicar en la disminución de la demanda agregada, lo que incentivaría a las empresas a asumir costos más elevados a fin de minimizar los daños. Se necesitan más estudios para precisar la extensión de esos daños y verificar si otras legislaciones con disposiciones análogas producen efectos similares en otras jurisdicciones.

El segundo eje del discurso contrario al exceso excepcional, a su vez, consiste en el cuestionamiento de los beneficios alegados de esa medida: su necesidad y su eficacia no habrían sido demostradas empíricamente de forma conclusiva y sería probable que de ella resultara la migración de los criminosos para otras plataformas. Conjugado al eje anterior, ese discurso entiende el acceso excepcional como una medida desproporcionalmente dañosa y potencialmente ineficaz. La primera alegación se ampara en la ausencia de datos o estudios que evalúen el efecto de la implementación de cifrado fuerte en plataformas y dispositivos sobre los índices de éxito en la resolución de investigaciones criminales. La segunda, a su vez, exige nuevos estudios, que deberán investigar los efectos de la implementación de mecanismos de acceso excepcional sobre la actividad criminosa en plataformas.

5.2. Sobre las alternativas al acceso excepcional

Cuanto a posibles métodos o técnicas alternativas para facultar a las autoridades el acceso a las informaciones demandadas sin comprometimiento del cifrado, se percibió que se levantaron dos conjuntos principales de soluciones potenciales: uno basado en la rotura de la seguridad de las informaciones en una de las puntas por la autoridad estatal

65 BARKER, George. LEHR, William. LONEY, Mark. SICKER, Douglas. O impacto econômico das leis que enfraquecem a criptografia. **Law & Economics Consulting Associates** (LECA). Tradução de Paulo Rená da Silva Santarém. 2021. Disponible en: https://isoc.org.br/noticia/o-impacto-economico-das-leis-que-enfraquecem-a-criptografia . **Acceso** el : 04/08/2021.

y otro basado en la cooperación con las empresas proveedoras de tecnología en las que las informaciones están almacenadas o se comunican.

En el primer conjunto, se levantó inicialmente la posibilidad de aprensión y desbloqueo de los dispositivos relevantes. Si por un lado, tal solución ofrece el beneficio de no interferir en el cifrado empleada en el sistema, es necesario reconocer que carga en si misma repercusiones significativas sobre los derechos de los ciudadanos, sobre todo en lo que se refiere a la protección de datos personales almacenados en dispositivos y a las condiciones de alejamiento legítimo del sigilo de datos estáticos. Tales impactos fueron notados por los entrevistados, que expresaron la preocupación con la posibilidad de violación excesiva de la intimidad en la medida en que los dispositivos muebles de un individuo presumiblemente contienen informaciones que extrapolan en mucho lo que es relevante para las investigaciones.

Se coloca, entonces, la cuestión de la legitimidad de la obligación judicial a la entrega de contraseña . A ese respecto, la sexta turma del STJ ha firmado entendimiento de que el llamamiento judicial al desbloqueo del dispositivo es legítimo. Sin embargo, inexiste obligación de información de la contraseña por parte del investigado en virtud del postulado constitucional de no permiso a la autoincriminación[66]. En reconsideración de voto, el relator, ministro Nefi Cordeiro, consideró que “es válido el orden judicial de entrega de las contraseñas de los dispositivos electrónicos aprendidos, pero el acusado no es obligado a proveer esas contraseñas, y ni debe sufrir sanciones”.

En conformidad a ese precedente, por lo tanto, el acceso al contenido del dispositivo aprehendido demandaría el recurso a métodos y herramientas direccionadas hacia la seguridad ofensiva. Eso levanta el debate sobre el uso de *lawful hacking* o *hacking gubernamental* para comprometimiento de una de las puntas del canal cifrado. Como evidenciado por el análisis de las entrevistas, aunque esos términos se usen genéricamente para designar el uso de recursos y métodos direccionados hacia la exploración de vulnerabilidades, el universo de recursos y métodos puede variar enormemente, una vez que el concepto abarca enfoques tan distintos como ingeniería social y el uso de *spyware* para obtención del acceso deseado.

Una vez que no poseen previsión expresada en el derecho procesual penal brasileño, las prácticas de *hacking* gubernamental han sido discutidas primariamente en el Poder Legislativo, donde se estableció un grupo de trabajo destinado a la elaboración de un anteproyecto de reforma del Código de Proceso Penal. En el texto sustitutivo que viene fundamentando los trabajos del referido GT hasta la fecha de finalización de este paper[67],

66 BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus nº 580.664 - RJ**. Rel. Ministro Nefi Cordeiro. Brasília, 20 out. 2020. Disponible en: https://stj.jusbrasil.com.br/jurisprudencia/1206242995/habeas-corpus-hc-580664-rj-2020-0111177-4/inteiro-teor-1206243005 . Acceso el: 05 ago. 2021

67 BRASIL. Câmara dos Deputados. **Parecer do Relator, Dep. João Campos (REPUBLIC-GO) da Comissão Especial destinada a proferir parecer ao Projeto de Lei nº 8045, de 2010, do Senado Federal, que trata do “Código de Processo Penal” (revoga o Decreto-Lei nº 3.689, de 1941. Altera os Decretos-Lei nº 2.848, de 1940; 1.002, de 1969; as Leis**

se contempla la materia en dos hipótesis de obtención de prueba: a "recolección remota, oculta o no, de datos en reposo accedidos a distancia" y la "recolección por acceso forzado de sistema informático o de redes de datos".

El tenor genérico de esas proposiciones hace resonar preocupaciones descriptas en la relatoría de acompañamiento sobre cifrado y anonimato publicada por el Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y Expresión en 2018. El documento alerta para una tendencia de los Estados a normatizar las prácticas de *hacking* a través de autorizaciones legales redactadas en "lenguaje impreciso y ambiguo, suministrando a las autoridades amplios poderes con supervisión externa mínima"[68]. A fin de enfocar tales riesgos , la relatoría recomienda que el recurso al *hacking* gubernamental se autorice solo en circunstancias excepcionales, observados los requisitos de legalidad, necesidad, proporcionalidad y finalidad legítima, cuya existencia se debe atestar casuísticamente por un órgano judicial independiente e imparcial[69].

Similarmente, un informe producido por el centro de referencia en derechos digitales *Access Now* sobre la materia, en 2016[70], recomienda una prohibición preventiva del *hacking* gubernamental en razón de sus riesgos para los derechos humanos. El documento recomienda que eventuales autorizaciones se adecuen a parámetros de notificación del usuario, transparencia, supervisión pública, integridad de sistemas, cooperación internacional, medicamento efectivo y salvaguardas contra el acceso ilegítimo, en adición a los propuestos por la relatoría de ONU.

El segundo conjunto principal de alternativas al cifrado difiere del primero en la medida en la que se apoya en prácticas de cooperación con la plataforma. En ese ámbito, las principales posibilidades levantadas fueron el uso de métodos de usuario o llave fantasma y de sistemas de escaneo del cliente (*client-side scanning*).

El debate sobre propuestas de usuario o llave fantasma ha ganado tracción reciente en a causa de un artículo publicado por dos directores técnicos de *Government Communications Headquarters*, principal autoridad del Reino Unido[71]. Los autores defienden que la

nº 4.898, de 1965, 7.210, de 1984; 8.038, de 1990; 9.099, de 1995; 9.279, de 1996; 9.609, de 1998; 11.340, de 2006; 11.343, de 2006), e apensados ao Projeto de Lei nº 8.045, de 2010. Portal da Câmara dos Deputados. Brasília, 26 abr. 2021. Disponible en: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/gt-anteprojeto-do-novo-codigo-de-processo-penal/documentos/outros-documentos/substitutivo-relator-joao-campos. Acceso el: 05 ago. 2021. p. 481.

68 ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Relatoria de acompanhamento sobre criptografia e anonimato do Relator Especial para a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão.** Genebra, 2018. Disponible en :https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf. Acceso el: 05 ago. 2021. p. 8.

69 ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Relatoria de acompanhamento sobre criptografia e anonimato do Relator Especial para a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão.** Genebra, 2018. Disponible en:https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf. Acceso el: 05 ago. 2021. p. 18.

70 STEPANOVICH, Amie et al. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponible en:https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf. Acceso el: 05 ago. 2021.

71 LEVY, Ian. ROBINSON, Crispin. Principles for a More Informed Exceptional Access Debate. **Lawfare - Hard National Security Choices**, 29 nov. 2018. Disponible en: https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate . Acceso el 05 ago. 2021.

incorporación velada de un tercero a las conversas de los investigados como mecanismo para el acceso a informaciones necesarias a las investigaciones no interferiría en el cifrado, lo que haría de ella una salida viable para el debate sobre *Going Dark*.

La propuesta repercutió negativamente en la comunidad de la seguridad de la información, resultando en una carta abierta[72] de respuesta firmada por 23 organizaciones de la sociedad civil del campo de los derechos digitales, 7 empresas de tecnología y comercio y 17 especialistas en seguridad digital y su gobernanza globalmente reconocidos en el campo académico. En la carta, los signatarios afirman que la propuesta de llave fantasma "crearía riesgos de seguridad digital al minar sistemas de autenticación cifrada, introducir vulnerabilidades potenciales y crear nuevos riesgos de abuso y uso indebido de esos sistemas" (traducción libre). Tal posicionamiento fue reiterado en una plantilla de hechos sobre la propuesta producida por *Internet Society*[73]. Similarmente, un artículo de opinión escrito por el científico de la computación y jurista Ross Schulman ha cuestionado la premisa fundamental de que tal método no representaría una interferencia en el cifrado. En sus palabras:

> En su propuesta, Levy y Crispin afirman que la propuesta de llaves fantasmas no "tocaría" el cifrado. Esa afirmación simplemente no es verdadera según ninguna definición normal de "cifrado". Mientras el método propuesto puede ni siempre involucrar modificaciones en los algoritmos criptográficos fundamentales [...], requeriría "tocar" y modificar las llaves cifradas. Los procesos de distribución y autenticación de las llaves son en sí mismos partes integrales de la totalidad del sistema cifrado. Debilitarlos tiene un impacto similar a debilitar el mismo algoritmo en lo que se refiere a la seguridad[74] (traducción libre).

El autor observa que la implementación de esos servicios exigiría alteraciones en los sistemas en escala masiva para producir un mecanismo de incorporación de llave a ser activado en dispositivos específicos bajo demanda. Los impactos resultantes serían similares a los de un sistema de custodia de llaves: aumento de la complejidad del sistema y reducción correspondiente de su seguridad, posibilidad de exploración por terceros maliciosos y reducción de la confianza en la plataforma. Por esas razones, se concluye que las propuestas de implementación de usuario o llave fantasma constituyen otro mecanismo de acceso excepcional y comportan riesgos y problemas técnicos, sociales, jurídicos, políticos y económicos análogos.

---

72 BRADFORD, Sharon. THOMPSON, Andi Wilson. Open Letter to GCHQ on the Threats Posed by the Ghost Proposal. **Lawfare - Hard National Security Choices**, 30 may. 2019. Disponible en: https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal. Acceso el: 05 ago. 2021.

73 INTERNET SOCIETY. Fact Sheet: Ghost Proposals. **Internet Society**, 24 mar. 2020. Disponible en: https://www.internetsociety.org/resources/doc/2020/fact-sheet-ghost-proposals/. Acceso el: 06 ago. 2021.

74 SCHULMAN, Ross. Why the Ghost Keys 'Solution' to Encryption is No Solution. **Just Security**, 18 jul. 2019. Disponible en: https://www.justsecurity.org/64968/why-the-ghost-keys-solution-to-encryption-is-no-solution/. Acceso el : 05 ago. 2021.

Otra alternativa basada en la cooperación con las proveedoras de dispositivos y canales son los sistemas de escaneo del cliente, por veces también designados como filtrado en la punta (*endpoint filtering*). La propuesta también ha sido objeto de críticas en la comunidad de seguridad de la información en los últimos años. En una plantilla de hechos divulgada sobre el asunto, la *Internet Society*[75] observó que la propuesta elevaría la complejidad del sistema, ampliando la superficie de ataque explorable por atacantes maliciosos. Estos podrían monitorear e interferir en las comunicaciones de los usuarios a partir de la manipulación de la base de datos de contenido dañoso. Alertaba, todavía, para la posibilidad de eventuales usos abusivos de esa capacidad, como la censura política de la comunicación de contenidos legítimos.

En un posicionamiento público sobre el tema, la *Electronic Frontier Foundation* ha alertado para otros problema relacionados a la propuesta[76]: la base de datos probablemente sería almacenada en el servidor, que tendería a ser informado de los identificadores de cada imagen enviada por el usuario. Una vez que tal sistema fuese implementado, se le podrían incorporar funcionalidades análogas para facultar acceso a contenidos textuales a modo de combate a la desinformación. El potencial de utilización de ese tipo de mecanismo para acceso a contenidos de comunicaciones implicaría en un incentivo continuo a la ampliación indebida de la base de datos. En el límite, se podría incorporar la totalidad del diccionario a esa base, efectivamente posibilitando el descifrado total de los mensajes y nulificando el propósito del cifrado.

Con relación a los metadatos, el debate sobre su acceso ha sido un punto de menor controversia jurídica. El régimen de guarda de datos establecido por el Marco Civil de Internet parametriza las informaciones que deben ser almacenadas por los proveedores de servicios de internet, los cuales pueden ser accedidos por las autoridades competentes mediante determinación judicial. En conformidad a la lógica de minimización del tratamiento de datos asociada al principio de la necesidad de la LGPD, la recolección y el almacenamiento de los datos personales, incluso metadatos sobre cuentas y comunicaciones, se debe limitar al mínimo necesario para la realización de los objetivos del tratamiento.

Además, expertos han alertado para riesgos asociados a la construcción de grafos sociales proyectados a partir de metadatos, como su monetización indebida por plataformas y el uso para mapeo de redes sociales de disidentes políticos, periodistas y activistas[77]. En el contexto tecnoautoritario descripto previamente, tales preocupaciones adquieren mayor gravedad, lo que refuerza la necesidad de minimización en la recolección

75 INTERNET SOCIETY. Fact Sheet: Client-Side Scanning. **Internet Society**, 24 mar. 2020. Disponible en: https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/. Acceso el: 06 ago. 2021.

76 PORTNOY, Erica. Why Adding Client-Side Scanning Breaks End-To-End Encryption. **Electronic Frontier Foundation**, 1 nov. 2019. Disponible en: https://www.eff.org/pt-br/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption. Acceso el: 06 ago. 2021.

77 INTERNET SOCIETY. Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India. **Internet Society**, 27 nov. 2020. Disponible el: https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india/. Acceso el: 06 ago. 2021.

y almacenamiento de los metadatos y la coherencia de los parámetros determinados por el Marco Civil de Internet con tal perspectiva de advertencia.

Por otro lado, ante la presión por la moderación de contenidos en ambientes cifrados, algunos estudiosos han considerado el análisis de metadatos como una alternativa menos invasiva que las demás. En un informe reciente sobre el tema[78], el *Center for Democracy and Technology* ha considerado tal método como apto a preservar la privacidad del usuario y del cifrado, siempre y cuando el análisis ocurra exclusivamente en el dispositivo del usuario y no implique en acceso a contenidos descifrados.

Para además de esos apuntes relativos a propuestas específicas, el examen de los enunciados de los entrevistados acerca de las alegadas alternativas al acceso excepcional evidencia una racionalidad sociotécnica que reconoce las estructuras técnicas de los sistemas cifrados como indisociables de las connotaciones políticas que adquirieron a lo largo de los años en lo que se refiere a la defensa de los derechos humanos, como privacidad y libertad de expresión. Por ese motivo, las alegadas alternativas - a ejemplo del escaneo del cliente y del análisis de metadatos - enfrentan variados grados de resistencia aunque su implementación no implique necesariamente en una interferencia directa en el algoritmo criptográfico o gestión de llaves.

5.3. Sobre los bloqueos de WhatsApp en Brasil y su relación con el Marco Civil de Internet

Los entendimientos de los entrevistados acerca de los bloqueos de WhatsApp y de su relación con el Marco Civil de Internet evidenciaron diferentes interpretaciones del contenido de la ley. La polémica jurídica se refiere específicamente al capítulo III, sección II, del referido diploma legal. Tales dispositivos, en resumen, disponen sobre el régimen aplicable a las operaciones de recolección, almacenamiento , guarda y tratamiento de registros, de datos personales o de comunicaciones realizadas en territorio nacional. Involucran también cuándo tales actividades son realizadas por persona jurídica con sede en el exterior, siempre y cuando ofrezca servicios para el público brasileño y posea como mínimo una integrante de su grupo económico con sede en territorio nacional.

A ese respeto, cumple destacar que el art. 10 preconiza que la guarda y la oferta de esas informaciones deben preservar la imagen, la vida privada, la honra y la intimidad de las partes involucradas. El art. 11, a su vez, condiciona tales actividades al respecto de la “legislación brasileña y a los derechos a la privacidad, a la protección de los datos

78 KAMARA et al. **Outside Looking In**: Approaches to Content Moderation in End-to-End Encrypted Systems. Center for Democracy and Technology Research, Washington, ago. 2021. Disponible en: https://cdt.org/insights/outside-looking-in-approaches-to-content-moderation-in-end-to-end-encrypted-systems/. Acceso em: 26 ago. 2021.

personales y al sigilo de las comunicaciones privadas y de los registros"[79]. El art. 12, por fin, establece sanciones para el no cumplimiento de los arts. 10 y 11. Los incisos III y IV de ese dispositivo, además, prevén las determinaciones de suspensión temporaria de las actividades referentes al art. 11 o la prohibición de ejercicio de esas actividades.

En lo que se refiere a la interpretación de esos dispositivos, se levantan dos tesis principales. La primera de ellas considera las sanciones del artículo 12 inaplicables a casos de no cumplimiento de órdenes judiciales de entrega de datos en razón de ese no cumplimiento no implicar en violación a la privacidad y a la protección de datos – por el contrario, cuando decurrente de implementación cifrada, tal inobservancia decorrería del éxito en proteger tales derechos. Tal interpretación se basa en las referencias expresadas en los artículos en cuestión a la defensa de esos derechos, como también al compromiso más general del MCI como la defensa de la privacidad. Se trata de lectura similar a una racionalidad comprometida primariamente con la defensa de la privacidad y refractaria al acceso excepcional y a medidas vistas como invasivas de la privacidad en general.

La segunda tesis, por otro lado, ve tales sanciones como aplicables a los casos en cuestión por entender que tales no cumplimientos implican en una violación del artículo 11. Eso porque la redacción del artículo 11 establecería el respeto a la legislación brasileña como un deber autónomo en relación al deber de observancia de la privacidad y de la protección de datos. Así, al no cumplir un orden judicial adecuadamente fundamentada y emitida por una autoridad competente, las empresas estarían infringiendo el ordenamiento nacional y se quedarían consecuentemente sujetas a la suspensión de sus servicios en los términos del art. 12. Esa posición se conecta a una racionalidad que ve las guerras criptográficas primariamente como un conflicto político entre Estados y empresas globales de tecnología y se compromete con la reafirmación de la autoridad estatal delante de la amenaza puesta por tales empresas a la referida autoridad. Tal tesis fue, incluso, uno de los fundamentos del tercer intento de bloqueo (segundo bloqueo concretizado) de WhatsApp en Brasil.

En la apreciación del mérito de esas interpretaciones, conviene reiterar inicialmente que, según previamente argumentado, la existencia de un deber de aptitud a la rotura de sigilo aplicable a las empresas de tecnología y a los proveedores de aplicaciones de internet en el derecho brasileño no es evidente. Así, se pone la cuestión de la licitud de la fijación de sanciones al agente económico que no cumple un orden judicial de entrega de datos en razón de, actuando de forma lícita, haber producido una arquitectura informacional que lo torna inapto a la rotura de sigilo. A ese respeto, la quinta turma del STJ ha confirmado la decisión del Ministro Ribeiro Dantas en el Recurso Especial Nº 1871695 – RO (2020/0095443-3), que alejó tal posibilidad por entender que nadie debe ser obligado a hacer el imposible y que los beneficios del cifrado superan em mucho sus eventuales cargas para la sociedad[80].

79 BRASIL. **Lei 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. DF: Presidência da República, 2014. Disponible en: www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acceso el: 05 ago. 2021.

80 BRASIL. Superior Tribunal de Justiça. **Terceira Seção afasta multa contra empresa que alega impossibilidade**

En ese sentido, también importa destacar el entendimiento de la Ministra Rosa Weber en su voto proferido en los autos de la Acción Declaratoria de Inconstitucionalidad (ADI) nº 5527. Según la Relatora, las referidas sanciones enunciadas del Marco Civil se prestan específicamente a regular sobre el no cumplimiento del deber de observancia de la legislación brasileña en actividades de tratamiento de registros, datos personales y comunicaciones. Los dispositivos en cuestión – y, en especial, las referidas sanciones legales –, aún según la Ministra, no se aplican en el contexto del no cumplimiento de órdenes judiciales.

Se concluye, entonces, que la inaplicabilidad de las sanciones en cuestión se encuentra respaldada tanto por el entendimiento de la relatora en ese caso, en que pese restar pendiente la conclusión del juicio del STF, cuando por la jurisprudencia del STJ.

Otro segmento de los entrevistados ha enseñado que, independiente de haber o no permiso legal en el Marco Civil de Internet que posibilite las órdenes de bloqueo, esas determinaciones judiciales serían posibles debido al llamado poder general de cautela del juez. Se trata de un mecanismo inicialmente previsto en el art. 798 del Código de Proceso Civil de 1973, por medio del cual el juez tendría el poder sin restricciones para aplicar medidas cautelares diversas de las previamente estipuladas en ley, a fin de garantizar el resultado útil del proceso.

Ese instrumento fue, de cierta forma, ampliado en el Código de Proceso Civil de 2015, en el cual se dejó de enunciar los métodos legalmente previstos de medidas cautelares. Alternativamente, el art. 301 enuncia el permiso general según el cual "la tutela de urgencia de naturaleza cautelar puede ser efectivada mediante arresto, secuestro, relación de bienes, registro de protesto contra alienación de bien y cualquier otra medida idónea para aseguración del derecho". La regla del proceso civil en el código vigente, en ese sentido, es integralmente centrada en el poder general de cautela del juez para determinar medidas cautelares y tutelas anticipadas durante el rito del proceso.

En el ámbito del Derecho Procesual Penal, el poder general de cautela del juez se firma por entendimiento jurisprudencial que trae la aplicabilidad subsidiaria del Código de Proceso Civil – y, por consecuencia, el enunciado del art. 301 de ese diploma legal – para el proceso penal. Se trata de interpretación decurrente del art. 3º del Código de Proceso Penal, que autoriza la "interpretación extensiva y la interpretación analógica, como también el suplemento de los principios generales de derecho". Con eso, el CPP permite el uso de institutos jurídicos externos al proceso penal para suplir eventuales lagunas legales.

Hay divergencia en la doctrina jurídica cuanto a la aplicabilidad del poder general de cautela del juez en sede de procesos criminales. Con todo, el entendimiento jurisprudencial mayoritario en el país se posiciona en el sentido de que se trata de prerrogativa necesaria

de interceptar mensagens criptografadas. 30/12/2020. Disponible en < https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/30122020-Terceira-Secao-afasta-multa-contra-empresa-que-alega-impossibilidade-de-interceptar-mensagens-criptografadas.aspx >, acceso el 03 ago 2021.

a la actividad del aplicador de la ley – sobre todo en lo que se refiere a las medidas cautelares no personales, es decir, diversas de aquellas aplicadas al reo en el curso del proceso penal. El poder de cautela, en ese sentido, transcurre de la teoría de los poderes implícitos del juez, en pro de la efectuación de la justicia. Se trata de una prerrogativa recurrentemente empleada, por ejemplo, para determinar multas diarias a las partes que dejan de atender a decisiones judiciales integrantes de la relación procesual que no sean el reo (al cual se aplican apenas las medidas cautelares expresamente previstas en ley) y que no cumplieron órdenes judiciales consideradas necesarias para la instrucción del proceso.

Con todo, en la imposición de medidas atípicas a través del poder de cautela del juez, es esencial que se observen preceptos de proporcionalidad y necesidad de la medida listada frente al objetivo deseado con la decisión. El examen de esos preceptos en el caso de los bloqueos de WhatsApp retoma un tema bastante discutido por los entrevistados: el entendimiento de que los bloqueos fueron injustificados en razón de su desproporcionalidad, más que ´por el Marco Civil de Internet.

En ese sentido, el impacto de las órdenes de bloqueo se coloca como central. Para diversos entrevistados, fue el daño resultante de los bloqueos del WhatsApp, más que la redacción del Marco Civil de Internet, que ocasionaba su ilegitimidad. Como se pudo constatar en la sección de este trabajo que describió los bloqueos, todas las órdenes de suspensión de la eficacia de los bloqueos tuvieron por fundamento el principio de la proporcionalidad. Todavía, dos de ellas entendieron que habría medios menos gravosos de garantía de la efectuación de la ley. En ese sentido, aunque esté pendiente la posición del STF en el contexto de las acciones que discuten los casos, el examen de las cuatro decisiones de suspensión de los bloqueos sugiere que los requisitos de necesidad (habría medios menos gravosos disponibles) y proporcionalidad (el daño resultante fue difuso y excesivo) no estarían presentes.

Así, el análisis de los bloqueos de WhatsApp y de su relación con el Marco Civil de Internet nos lleva a tres conclusiones: i) tesis restrictiva de las sanciones previstas en el art. 12 del Marco Civil de Internet a violaciones a la privacidad y a la protección de datos se respalda por el entendimiento de la ministra Rosa Weber, pendiente la conclusión del juicio, de modo que el artículo 11 no podría fundamentar los bloqueos; ii) el poder general de cautela del juez tampoco podría fundamentar adecuadamente los bloqueos, a la vista de que ausentes los requisitos de proporcionalidad y necesidad, según evidenciado por las órdenes de suspensión de los bloqueos; iii) sanciones económicas también no se podrían aplicar, según entendimiento firmado por STJ, en razón de la imposibilidad fáctica de entrega de los datos aliada al equilibrio de los costos y beneficios del cifrado, que legitima la manutención del cifrado en el sistema.

6. Conclusión

La interlocución con los más de 40 profesionales entrevistados para la realización del presente estudio ha evidenciado la multiplicidad de dimensiones y perspectivas que cruzan el debate sobre las políticas del cifrado en el siglo XXI, en especial en lo que toca a las guerras criptográficas. Aunque esa complejidad imposibilite una investigación exhaustiva de todos los aspectos de la controversia en cuestión, el análisis sistemático del contenido de las entrevistas ha resultado una cartografía de sus principales elementos contenciosos, como también de los presupuestos valorativos y fácticos que fundamentan los posicionamientos de los actores. A partir de ese mapeo, se examinaron las relaciones entre las percepciones de los actores y los contextos socioeconómicos, jurídicos, políticos y técnicos con los que se relacionan objetivamente.

Durante las fases I y II de las guerras criptográficas, el núcleo de la controversia ha sido por veces identificado con la cuestión del acceso excepcional a contenidos protegidos por cifrado fuerte. En los enunciados analizados, se observó que la defensa de medidas de ese tipo se articula a una racionalidad de cuño esencialmente político-jurídico. Sus presupuestos fundamentales son la primacía de la seguridad - entendida como el éxito en la persecución penal, sobre todo tratándose de crímenes graves - sobre la privacidad y la existencia de un deber de aptitud a la rotura de sigilo aplicable a las empresas de tecnología y proveedoras de aplicación. Todavía, entiende la creencia en la confiabilidad de los controles institucionales como un principio normativo cuya aceptación es necesaria al funcionamiento del Estado, bajo riesgo de descualificación de toda la institucionalidad, y de ella infieren mitigables los riesgos de abuso de la herramienta por la autoridad pública.

El discurso contrario al acceso excepcional, a su vez, adopta un énfasis distinto. Por un lado, argumenta que los daños de la medida son excesivos en los planes técnico (reducción de la seguridad del sistema), jurídico-político (desproporcionalidad, riesgos a los derechos de los usuarios y daños a la confianza en el ambiente digital) y económico (cargas demasiadas a los proveedores y perjuicio a toda la economía digital). Por otro, cuestiona la eficacia y la necesidad de la medida, argumentando que no es posible saber hasta qué punto el cifrado efectivamente contribuye para el fracaso investigativo y que es probable que los criminosos atacados evadirían la plataforma debilitada.

El mapeo de los argumentos que permean esos discursos visibiliza la existencia de premisas jurídicas y fácticas pasibles de examen hermenéutico o empírico, lo que puede contribuir significativamente para la madurez del debate. El análisis presentado ha evidenciado, por ejemplo, que la existencia de un deber de aptitud a la rotura de sigilo aplicable a los sectores de tecnología y de aplicaciones digitales en Brasil es, como mínimo, jurídicamente contestable. Similarmente, ha demostrado que las preocupaciones con los daños del acceso excepcional encuentran respaldo teórico en la ciencia cifrada y empírico en estudios sobre el ambiente político brasileño y sobre los impactos económicos de normas restrictivas del cifrado.

Por otro lado, ha verificado que hay obstáculos metodológicos a una medición cualificada de la alegada banalización de las roturas de sigilo en el país – aunque el crecimiento explosivo en el volumen de roturas sea un fenómeno digno de nota en sí mismo. Todavía, llama atención para la necesidad de estudios que investiguen la dimensión efectiva del alegado obstáculo representado por el cifrado en el éxito de la investigación criminal e investiguen el lastro empírico de la tesis de la migración de la criminalidad a causa de la implementación de acceso excepcional.

Aunque esa cualificación pueda surtir efectos positivos sobre el debate, la contraposición entre las énfasis y las premisas ético-políticas de las dos racionalidades expuestas también sugiere que la simple verificación factual de las alegaciones de los dos lados tiene un potencial limitado de resolución de la controversia establecida. Eso porque los puntos de vista de los actores se insieren en narrativas, actitudes y disposiciones afectivas más generales sobre las relaciones entre Estado e individuo, entre privacidad y seguridad. La defensa del acceso excepcional trata la confiabilidad de los controles institucionales como un principio normativo, al paso que la oposición a tal medida tiene como principio el escepticismo sobre la eficacia de esos controles. Un lado asocia la seguridad a imágenes de persecución penal eficaz, el otro a plataformas tecnológicas diseñadas teniendo como objetivo la máxima protección de las informaciones traficadas. Un lado ve la actuación represiva del Estado como fundamentalmente garantizadora del interés público, el otro la ve como altamente pasible de instrumentalización política contra las libertades democráticas.

Tomemos como ejemplo la tesis de que hay un deber de aptitud a la rotura de sigilo aplicable a los sectores de tecnología y de aplicaciones digitales en Brasil. Su contestación difícilmente resolvería la controversia: los defensores del acceso excepcional podrían simplemente replicarla, movilizando otros argumentos jurídicos para fundamentar la existencia de tal deber, o, alternativamente, desplazar el debate del plan descriptivo al plan normativo, defendiendo que si tal deber inexiste, debería pasar a existir por fuerza de ley o jurisprudencia superior.

Eso porque su posición supone, para además de la cuestión específica sobre la existencia de esa previsión en el ordenamiento brasileño, ser fundamentalmente inaceptable que existan espacios comunicativos inaccesibles a los ojos de la autoridad estatal.

Eso es similarmente corroborado por el examen de las controversias involucrando las alegadas alternativas al acceso excepcional. Propuestas como escaneo del cliente, *hacking* gubernamental y uso extensivo de metadatos tienden a encontrar enorme resistencia entre activistas y académicos de los derechos digitales. Aunque no interfieran necesariamente en el algoritmo utilizado ni en los procesos de generación y gestión de llaves -, tales soluciones se ven como minando el cifrado porque atingen los valores que el empleo del cifrado convencionalmente busca proteger. De esa forma, se observa que la defensa del cifrado se conecta a preocupaciones más amplias como la protección de la privacidad, de la libertad de expresión, de los derechos políticos y valores democráticos,

en un contexto en el que estos son amenazados por la criminalidad cibernética y por la vigilancia estatal. En ese prisma, se ve la ampliación de la vigilancia como un ataque a la cifrado aunque no involucre interferencia en el sistema criptográfico en sentido estricto.

Del mismo modo, la controversia en torno a la interpretación de los arts. 10, 11 y 12 del Marco Civil de la Internet evoca ese disenso más profundo sobre los valores que deben orientar la interpretación de la ley. La interpretación contraria a los bloqueos enfatiza los trechos protectores de la privacidad y de la protección de datos personales de los dispositivos precisamente por ser esos los valores fundamentales que tal racionalidad encampa. Por otro lado, la interpretación favorable a los bloqueos enfatiza la obligación de respecto a la legislación brasileña porque sus preocupaciones primarias son con la amenaza puesta por las empresas globales de tecnología a la autoridad estatal, que se encuentran en la posición de desafiar en razón de su poder económico transnacional. De las perspectivas de ambos los actores, lo que está en cuestión es más profundo que la redacción de esos dispositivos específicos.

A lo largo de este estudio, se objetivó presentar las dimensiones argumentativas que impregnan el debate actual entre la seguridad pública y la defensa estatal versus los derechos a la privacidad y a la libertad de expresión en el medio digital – bajo el cerne de la utilización de técnicas de cifrado fuerte. Se trata de un debate duradero, cerrado desde al menos la segunda mitad del siglo XX, y que permanece esencialmente perene desde entonces. Con todo, se percibe, que se trata de una cuestión más profunda de lo que se observa en primer análisis: los argumentos en favor de ambos los posicionamientos adquieren dimensiones múltiples, que extravasan la propria legitimidad del cifrado. Las múltiples faces de esa discusión– sociales, políticas, jurídicas, entre otras – no pueden, por lo tanto, ser consideradas individualmente en pro de la resolución completa de la controversia.

Se buscó, finalmente, ofrecer una contribución sobre las perspectivas que integran el debate sobre el uso de la cifrado. Se espera que el mapeo de los datos de los entrevistados, como también el análisis de esos pronunciamientos a la luz de los mecanismos jurídicos vigentes en Brasil, se puedan utilizar para una cualificación más profunda del debate en pauta a partir de estudios futuros.

7. Referencias bibliográficas

ABELSON, Hal *et al*. Keys under doormats: mandating insecurity by requiring government access to all data and communications. **Journal of Cybersecurity**, v. 1, n. 1, p. 69-79, 2015. p.69.

ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, nº 3, 2017, p. 24-42. p. 29.

ABREU, Jaqueline. Audiência Pública sobre Criptografia e Bloqueios do WhatsApp: argumentos diante do STF. 26/06/2017. Bloqueios.info . Disponible en: <http://bloqueios.info/pt/audiencia-publica-sobre-criptografia-e-bloqueios-do-whatsapp-argumentos-diante-do-stf/ >, acceso el 02 ago 2021.

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. **Vigilância sobre as comunicações no Brasil**: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017. p. 44-45

AGÊNCIA CÂMARA DE NOTÍCIAS. **Relatório preliminar do novo CPP incorpora provas digitais e novas tecnologias ao processo criminal.** Relator: Deputado João Campos. 13/04/2021. Disponible em: <https://www.camara.leg.br/noticias/745824-relatorio-preliminar-do-novo-cpp-incorpora-provas-digitais-e-novas-tecnologias-ao-processo-criminal/ >, acceso el 26 ago. 2021.

ALMEIDA, Frederico de. MONTEIRO, Filipe Jordão; SMIDERLE, Afonso.a criminalização dos protestos do movimento passe livre em são paulo (2013-2015). **Revista Brasileira de Ciências Sociais** [online]. v. 35, n. 102, 2020.

ANTONIALLI, Dennys. M.;ABREU, Jacqueline; MASSARO, Heloisa. M. M. ; LUCIANO, Maria. Acceso de autoridades policiais a celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais. **Revista Brasileira de Ciências Criminais**, v. 154, p. 177-214, 2019.

ARTIGO 19. **As restrições ao direito de protesto no Brasil**. 5 anos de junho de 2013: Como os três poderes intensificaram sua articulação e sofisticaram os mecanismos de restrição ao direito de protesto progressivamente. Artigo 19, 2018. Disponible en: https://artigo19.org/5anosde2013/. Acceso em: 04/08/2021.

ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA; CENTRO DE ANÁLISE DA LIBERDADE E DO AUTORITARISMO (LAUT). **Retrospectiva - Tecnoautoritarismo 2020. LAUT,** 2021. Disponible en: https://laut.org.br/wp-content/uploads/2021/01/RETROSPECTIVA-TECNOAUTORITARISMO-2020.pdf. Acceso em: 04/08/2021.

BARKER, George. LEHR, William. LONEY, Mark. SICKER, Douglas. O impacto econômico das leis que enfraquecem a criptografia. **Law & Economics Consulting Associates** (LECA). Tradução de Paulo Renà da Silva Santarém. 2021. Disponible en: https://isoc.org.br/noticia/o-impacto-economico-das-leis-que-enfraquecem-a-criptografia . Acceso em: 04/08/2021.

BARIFOUSE, R.; DUARTE, F.; BARRUCHO, L. G. Liberação do WhatsApp não encerra polêmica disputa com Justiça brasileira. **G1**. Tecnologia e Games. Disponible en: http://g1.globo.com/tecnologia/noticia/2015/12/liberacao-do-whatsapp-nao-encerra-polemica-disputa-com-justica-brasileira.html. Acceso em: 29/07/2021.

BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY (BERKMAN). **Não Entre em Pânico**: Avançando no debate sobre "obscurecimento" (Going Dark). 2018. Tradução pelo Instituto de Tecnologia e Sociedade do Rio. Disponible en: https://itsrio.org/wp-content/uploads/2018/10/Dont_Panic_Making_Progress_on_Going_Dark_Debate_PT.pdf Acceso em 02/08/2021.

BONI, V.; QUARESMA, S. J. Aprendendo a entrevistar: como fazer entrevistas em Ciências Sociais. **Em Tese - Revista Eletrônica dos Pós-Graduandos em Sociologia Política da UFSC**, Florianópolis, v. 2, n. 1 (3), p. 68-80, jan./jul. 2005.

BRADFORD, Sharon. THOMPSON, Andi Wilson. Open Letter to GCHQ on the Threats Posed by the Ghost Proposal. **Lawfare - Hard National Security Choices**, 30 mai. 2019. Disponible en: https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal. Acceso em: 05 ago. 2021.

BRASIL. **Lei 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. DF: Presidência da República, 2014. Disponible en: www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acceso em: 05 ago. 2021.

BRASIL. Juízo de Direito da Vara Criminal da Comarca de Lagarto. **Processo nº 201655090143**. Decisão. Juiz Marcel Maia Montalvão. Lagarto, Sergipe, 26 abr. 2016.

BRASIL. Tribunal de Justiça do Estado de Sergipe. **Mandado de Segurança nº 201600110899**. Decisão liminar. Rel. Des. Ricardo Múcio Santana de Abreu Lima. Aracaju, 3 mai. 2016. Disponible en: <http://www.omci.org.br/m/jurisprudencias/ arquivos/2016/tjse_201600110899_03052016.pdf> Acceso em: 2 nov. 2016.

BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Inquérito Policial nº 062-00164/2016**. Juíza Daniela Barbosa Assumpção de Souza. Duque de Caxias, RJ, jul. 2016. Disponible en: <https://drive.google.com/file/d/0Bw3seZUv__5ubnFudjUwMm9OZGc/view>. Acceso em: 30/07/2021

BRASIL. Conselho Nacional de Justiça (CNJ). Sistema Nacional de Controle de Interceptações Telefônicas. **CNJ**, Brasília, 2021. Disponible en: https://www.cnj.jus.br/sistemas/sistema-nacional-de-controle-de-interceptacoes-telefonicas/. Acceso em: 04/08/2021.

BRASIL. Tribunal de Justiça do Estado de São Paulo. **Mandado de Segurança nº 2271462-77.2015.8.26.0000**. Decisão liminar. Rel. Des. Xavier de Souza. São Paulo, 17 dez. 2015. Disponible en: http://www.omci.org.br/m/jurisprudencias/arquivos/2015/tjsp_2271462 7720158260000_17122015.pdf. Acceso em: 29/07/2021.

BRASIL. Central de Inquéritos da Comarca de Teresina. **Nota**. Juiz Luiz de Moura Correia. Teresina, 26 fev. 2015. Disponible en: http://s2.glbimg.com/MdNVliNDOaF45o27HM8_tsG3wll=/s.glbimg.com/jo/g1/f/original/2015/02/26/nota_juiz_whatsapp_ok.jpg. Acceso em: 29/07/2021.

BRASIL. Tribunal de Justiça do Estado do Piauí. **Mandado de Segurança nº 2015.0001.001592-4**. Rel. Des. Raimundo Nonato da Costa Alencar. Teresina, 26 fev. 2015. Disponible en: <http://www.migalhas.com.br/arquivos/2015/2/art20150227-03.pdf> Acceso em: 29/07/2021.

BRASIL. Superior Tribunal de Justiça. **Terceira Seção afasta multa contra empresa que alega impossibilidade de interceptar mensagens criptografadas.** 30/12/2020. Disponible en < https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/30122020-Terceira-Secao-afasta-multa-contra-empresa-que-alega-impossibilidade-de-interceptar-mensagens-criptografadas.aspx >, acceso em 03 ago 2021.

BRASIL.Superior Tribunal de Justiça. **Criptografia em aplicativo de mensagem não permite multa cominatória, decide Quinta Turma.** 24/06/2021. Disponible en <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/24062021-Criptografia-em-aplicativo-de-mensagem-nao-permite-multa-cominatoria--decide-Quinta-Turma.aspx>, acceso em 03 ago 2021.

BRASIL. Ministério da Justiça e Segurança pública. **Simpósio sobre Going Dark termina com declaração de 13 países.** Disponible en <https://www.justica.gov.br/news/collective-nitf-content-1550010028.2>, acceso em 03 ago 2021.

BRASIL. Supremo Tribunal Federal. **Medida cautelar de arguição de descumprimento de preceito fundamental**. Decisão liminar. Rel. Min. Ricardo Lewandowski. Brasília, 19 jul. 2016. Disponible en: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403MC.pdf. Acceso em: 30/07/2021.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental Nº 403.** Relator: Edson Fachin. Brasília, DF. Disponible en: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500. Acceso em: 06 ago. 2021.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade Nº 5527**. Relatora: Rosa Weber. Brasília, DF. Disponible en: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282. Acceso em: 06 ago. 2021.

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus Nº 51.531 - RO**. Rel. Ministro Nefi Cordeiro. Brasília, 09 mai. 2016. Disponible en: https://stj.jusbrasil.com.br/jurisprudencia/340165638/recurso-ordinario-em-habeas-corpus-rhc-51531-ro-2014-0232367-7/inteiro-teor-340165652. Acceso em: 05 ago. 2021.

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus nº 580.664 - RJ**. Rel. Ministro Nefi Cordeiro. Brasília, 20 out. 2020. Disponible en:https://stj.jusbrasil.com.br/jurisprudencia/1206242995/habeas-corpus-hc-580664-rj-2020-0111177-4/inteiro-teor-1206243005 . Acceso em: 05 ago. 2021

BRASIL. Juízo de Direito da Vara Criminal da Comarca de Lagarto. Processo nº 201655090143. **Decisão. Juiz Marcel Maia Montalvão**. Lagarto, Sergipe, 26 abr. 2016.

BRASIL. **Declaração do Going Dark Brasil.** Disponible en <https://www.justica.gov.br/news/collective-nitf-content-1550010028.2/documentos/declaracao-do-going-dark-brasil.pdf> acceso em 04 ago 2021.

BRASIL. Câmara dos Deputados. **Parecer do Relator, Dep. João Campos (REPUBLIC-GO) da Comissão Especial destinada a proferir parecer ao Projeto de Lei nº 8045, de 2010, do Senado Federal, que trata do "Código de Processo Penal" (revoga o Decreto-Lei nº 3.689, de 1941. Altera os Decretos-Lei nº 2.848, de 1940; 1.002, de 1969; as Leis nº 4.898, de 1965, 7.210, de 1984; 8.038, de 1990; 9.099, de 1995; 9.279, de 1996; 9.609, de 1998; 11.340, de 2006; 11.343, de 2006), e apensados ao Projeto de Lei nº 8.045, de 2010**. Portal da Câmara dos Deputados. Brasília, 26 abr. 2021. Disponible en: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/gt-anteprojeto-do-novo-codigo-de-processo-penal/documentos/outros-documentos/substitutivo-relator-joao-campos. Acceso em: 05 ago. 2021. p. 481.

CANABARRO, Diego. AULA 4 - Criptografia: experiências regulatórias e debates internacionais com Diego Canabarro. Belo Horizonte: **Instituto Iris,** 2021. (39 min.), son., color. Disponible en: https://youtu.be/EDaI5_z-hBo?t=2200. Acceso em: 25 ago. 2021.

CANTO, Mariana. RAMIRO, André. REAL, Paula C. Criptografia no STF: O que dizem os votos de Rosa Weber e Edson Fachin e o que podemos aprender com eles. **IP.Rec – Instituto de Pesquisa em Direito e Tecnologia do Recife.** Disponible en <https://ip.rec.br/2020/06/22/criptografia-no-stf-o-que-dizem-os-votos-de-rosa-weber-e-edson-fachin-e-o-que-podemos-aprender-com-eles/ >, acceso em 02 ago 2021.

CARVALHO, Thaís Bernardes. **O bloqueio judicial do WhatsApp no território brasileiro no contexto do Estado Democrático de Direito.** 2017. 69 f. Monografia de graduação

no curso de Direito - Universidade Federal de Lavras, Lavras, 2017; Disponible en http://repositorio.ufla.br/handle/1/30751. Acceso em 16 de agosto de 2021.

CRABTREE, B. & MILLER, W. **Doing qualitative research**. Thousand Oaks, Calif.: Sage Publications, 1999.

COALIZÃO PELOS DIREITOS NA REDE. **Reforma do Código de Processo Penal pode aumentar vigilância e precisa de equilíbrio em questões de tecnologia.** 20 de maio de 2021. Disponible en <https://direitosnarede.org.br/2021/05/20/reforma-do-codigo-de-processo-penal-pode-aumentar-vigilancia-e-precisa-de-equilibrio-em-questoes-de-tecnologia/>, acceso em 25 ago. 2021.

COMEY; James B. **Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?** Out. 2014, discurso realizado na Brookings Institution. [Online]. Disponible en https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course. Acceso em: 02 ago. 2021.

Couto Chaves Brandão. (Org.). **Tecnologias e conectividade**: direito e políticas na governança das redes. 1ed. Belo Horizonte: 2018, v. 1, p. 15-30.

DIFFIE, Whitfiead. HELLMAN, Marin. **New directions in cryptography.** IEEE Transactions on Information Theory, 22, 644-654.

DONEDA, Danilo. MACHADO, Diego. (coords.) **A criptografia no direito brasileiro**. São Paulo: Thompson Reuters - Revista do Tribunais, 2019.

FROOMKIN, Michael. The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. **University of Pennsylvania Law Review**, v. 143, n. 3, p. 709–897, 1995.

GASKELL, G. Entrevistas individuais e grupais. In: BAUER, M. W.; GASKELL, G. (Org.). **Pesquisa qualitativa com texto, imagem e som**: um manual prático. Petrópolis, RJ: Vozes, 2000, pp. 64-89.

Global Encryption Coalition. Brazilian Code of Criminal Procedure reform must not undermine encryption. June 28, 2021. Disponible en < https://www.globalencryption.org/2021/06/brazilian-code-of-criminal-procedure-reform-must-not-undermine-encryption/>, acceso em 25 ago. 2021.

GROVER, Gurshabad; RAJWADE, Tanaya; KATIRA, Divyank. The Ministry And The Trace: Subverting End-To-End Encryption, 14 NUJS Law Review. 1(2021). p. 2-6. Disponible en <http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption/ >. Acceso em: 02 ago. 2021.

HOBOKEN, J. V.; SCHULZ, W. **Human rights and encryption**. Paris: UNESCO, 2016.

INMAN, B. R. The NSA perspective on telecommunications protection in the nongovernamental sector. Cryptologia, v. 3, n. 3, 129 - 135, 1979.

INTERNET SOCIETY. Fact Sheet: Ghost Proposals. **Internet Society**, 24 mar. 2020. Disponible en: https://www.internetsociety.org/resources/doc/2020/fact-sheet-ghost-proposals/. Acceso em: 06 ago. 2021.

INTERNET SOCIETY. Fact Sheet: Client-Side Scanning. **Internet Society**, 24 mar. 2020. Disponible en: https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/. Acceso em: 06 ago. 2021.

INTERNET SOCIETY. Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India. **Internet Society**, 27 nov. 2020. Disponible en: https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india/. Acceso em: 06 ago. 2021.

JARVIS, Craig. **A New Crypto Wars Chronology (I)**. 21 fev. 2020. LinkedIn: Craig Jarvis. Disponible en: https://www.linkedin.com/pulse/new-crypto-wars-chronology-craig-jarvis/. Acceso em: 29 jul. 2021.

JARVIS, Craig. **A New Crypto Wars Chronology (II)**. 20 jul. 2020. LinkedIn: Craig Jarvis. Disponible en: https://www.linkedin.com/pulse/new-crypto-wars-chronology-ii-craig-jarvis/?articleId=6690894456150859776. Acceso em: 29 jul. 2021

JARVIS, Craig. Crypto Wars: The Fight for Privacy in the Digital Age: A Political History of Digital Encryption. CRC Press, 2020.

KAMARA et al. Outside Looking In: Approaches to Content Moderation in End-to-End Encrypted Systems. **Center for Democracy and Technology Research,** Washington, ago. 2021. Disponible en: https://cdt.org/insights/outside-looking-in-approaches-to-content-moderation-in-end-to-end-encrypted-systems/. Acceso em: 26 ago. 2021.

KRIPPENDORFF, K. **Content Analysis**: an introduction to its methodology. Thousand Oaks, Calif.: Sage Publications, 2004.

KURTZ, Lahis P.; MENEZES, Victor. A.. **Entre o direito e a força na sociedade da informação: bloqueio judicial do WhatsApp e ADI nº 5.527.** In: Fabrício Bertini Pasquot Polido; Lucas Costa dos Anjos; Luiza

LEVY, Ian. ROBINSON, Crispin. Principles for a More Informed Exceptional Access Debate. **Lawfare - Hard National Security Choices**, 29 nov. 2018. Disponible en: https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate . Acceso em 05 ago. 2021.

LIU, H. Inside the Black Box: Political Economy of the Trans-Pacific Partnership's Encryption Clause. Journal of World Trade, v. 51, n. 2, p. 309 - 334, 2017.

MASI, Carlos Velho. O caso Escher e outros v. Brasil e o sigilo das comunicações telefônicas. **Revista dos Tribunais**, v. 932, Junho de 2013, pp. 309-352

MITCHELL, Bonnie et al. Going Dark: Impact to Intelligence and Law Enforcement and Threat Mitigation. 2017.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Relatoria de acompanhamento sobre criptografia e anonimato do Relator Especial para a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão.** Genebra, 2018. Disponible en:https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf. Acceso em: 05 ago. 2021. p. 8.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Relatoria de acompanhamento sobre criptografia e anonimato do Relator Especial para a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão.** Genebra, 2018. Disponible en:https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf. Acceso em: 05 ago. 2021. p. 18.

PORTNOY, Erica. Why Adding Client-Side Scanning Breaks End-To-End Encryption. **Electronic Frontier Foundation**, 1 nov. 2019. Disponible en: https://www.eff.org/pt-br/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption. Acceso em: 06 ago. 2021.

QUEIROZ, Rafael Mafei Rabelo. PONCE, Paula Perdigoni. Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Internet & Sociedade**, v.1,n.1, fev/2020, p.64-90.

RAMIRO, André. CANTO, Mariana. REAL, P. C. et al. **O Mosaico Legislativo da Criptografia no Brasil: Uma Análise de Projetos de Lei**. IP.Rec. Disponible en <https://ip.rec.br/wp-content/uploads/2020/08/O-mosaico-legislativo-da-criptografia-no-Brasil-uma-an%C3%A1lise-de-Projetos-de-Lei-1.pdf >, acceso em 04 ago 2021.

RAY, Trisha. The Encryption Debate in India: 2021 Update. 2021.

RIDER, Karina. The Privacy Paradox: how market privacy facilitates government surveillance. **Information, Communication & Society**. v. 21, n. 10, p.1369-1385, abr. 2017.

RODRIGUES, G. R. A controvérsia cifrada: o Clipper e o mito da derrota estatal nas guerras criptográficas dos anos 1990. Em: ALVES, Marco Antônio Sousa. NOBRE, Marcio

Rimet. (orgs.). **A sociedade da informação em questão**: o direito, o poder e o sujeito na contemporaneidade. Belo Horizonte: D'Plácido, 2019.

ROSENTHAL, G. **Pesquisa social interpretativa**: uma introdução. Porto Alegre: Edipucrs, 2014.

SCHNEIER, Bruce. **Applied Cryptography**: Protocols, Algorithms, and Source Code in C. 20th Anniversary Edition. New Jersey: John Willey & Sons, 1996, p. 30.

SCHULMAN, Ross. Why the Ghost Keys 'Solution' to Encryption is No Solution. **Just Security**, 18 jul. 2019. Disponible en: https://www.justsecurity.org/64968/why-the-ghost-keys-solution-to-encryption-is-no-solution/. Acceso em: 05 ago. 2021.

SILVA JUNIOR, L. A.; LEAO, M. B. C. O software Atlas.ti como recurso para a análise de conteúdo: analisando a robótica no Ensino de Ciências em teses brasileiras. **Ciênc. educ.** (Bauru), Bauru , v. 24, n. 3, p. 715-728, set. 2018.

SINGH, Simon. **The Code Book**: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: First Anchor Books, 2000. p. 234-235.

STEPANOVICH, Amie et al. **A Human Rights Response to Government Hacking**. Access Now, set. 2016. Disponible en:https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf. Acceso em: 05 ago. 2021.

STILGHERRIAN. The Encryption Debate in Australia: 2021 Update. 2021.

VINUTO, J. A amostragem em Bola de Neve na pesquisa qualitativa: um debate em aberto. **Temáticas** (UNICAMP), v. 44, p. 201-218, 2014.

WHATSAPP INC. **Blog do WhatsApp**. Criptografia de Ponta-a-Ponta. 05 abr. 2016. Disponible en: https://blog.whatsapp.com/end-to-end-encryption. Acceso em: 30/07/2021

Apéndice 1 – Guión de la entrevista

Bloque I – Presentación y temas generales

1. ¿Cuántos años tiene?
2. ¿Dónde vive?
3. ¿Cuál su área de formación?
4. ¿A qué se dedica actualmente? (Cargo actual y atribuciones)
5. Cuéntenos un poco de su trayectoria profesional. (EXPLORAR: ¿Dónde ha trabajado? ¿Cuáles funciones ha ejercido? ¿Cómo ha sido el contacto con las cuestiones de internet y sociedad?)
6. ¿Cómo las transformaciones que trajo internet a la sociedad impactaron su trayectoria profesional?
7. Pensando en la transformaciones que trajo internet a la sociedad, ¿ hay algo que ud entienda como especialmente positivo o especialmente negativo?

Bloque II - Cifrado, privacidad y seguridad

8. En una escala de 0 a 10, ¿qué importancia ud. atribuye a la privacidad **en la sociedad actual**? ¿Por qué?
9. En una escala de 0 a 10, ¿qué importancia ud. atribuye **a su** privacidad? ¿Por qué?
10. ¿Cómo evalúa ud el debate público sobre privacidad hoy día? (EXPLORAR: Brasil, otros países etc)
11. ¿Cómo ve ud la relación entre privacidad y seguridad hoy día? (EXPLORAR: ¿hay contextos en los que esos valores entran en conflicto?)
12. En su percepción, ¿cuáles son las relaciones entre seguridad pública y seguridad de la información?
13. En una escala de 0 a 10, ¿qué importancia ud atribuye al cifrado **en la sociedad actual**? ¿Por qué?

14. En una escala de 0 a 10, ¿que importancia atribuye el cifrado **en las aplicaciones que usa?** ¿Por qué?

15. En una escala de 0 a 10, ¿cuál su nivel de satisfacción con el actual ambiente regulatorio sobre cifrado? ¿Por qué?

16. Si ud pudiera, ¿ cambiaría algo en ese ambiente? ¿Concretamente, qué?

17. En su entendimiento, ¿hay situaciones en las que el uso de cifrado entra en conflicto con el interés público? (Explorar diferentes entendimientos sobre el público)

18. ¿Ud apoyaría la introducción de un mecanismo de acceso excepcional en el cifrado para fines de investigación criminal? (Explorar: ¿Por qué? Si sí, ¿cuáles situaciones legítimas e ilegítimas para el uso de ese mecanismo? ¿Hay riesgos relacionados a eso? Si hay riesgos , ¿cuáles? ¿Hay costos económicos, reputacionales o sociales asociados? ¿Existe algún medio término?)

19. En su entendimiento, ¿es posible conciliar la seguridad de los usuarios con la introducción de un mecanismo de acceso excepcional en el cifrado?

20. ¿Cómo evalúa la legitimidad de los bloqueos de WhatsApp ocurridos en 2015 y 2016 en Brasil? (Explorar las dimensiones de la legitimidad)

21. **Para profesionales de Derecho:** En su entendimiento, ¿el Marco Civil de Internet autoriza bloqueos de aplicación por no cumplimiento de órdenes de entrega de datos para fines de investigaciones criminales?

22. ¿Conoce ud alguna alternativa para el acceso a esos datos que no involucre acceso excepcional? (Explorar: si sí, ¿cuáles? ¿cuáles los riesgos asociados a cada una?)

23. ¿Ha ud actuado profesionalmente en alguna situación que involucrara de alguna forma la cuestión del acceso a datos cifrados?

24. En su trabajo, ¿trata ud con cuestiones relacionadas a la regulación de cifrado de alguna manera?

25. **Para funcionarios federales/gestores públicos**: En su opinión, ¿los esfuerzos de modernización del servicio público y digitalización del gobierno vienen acompañados de una preocupación con seguridad de la información?

Bloco III – Capacitación y educación

26. Considerando aspectos técnicos y regulatorios, de cero a 10, ¿cuál nota atribuye ud a su grado de conocimiento sobre cifrado? ¿Por qué? (Explorar: ¿ hay lagunas? Si sí, ¿cuáles?)

27. ¿Ya ha realizado algún curso o capacitación direccionada hacia este tema? (Explorar: Si sí, ¿cuál fue la institución responsable? ¿Cuál la duración? ¿Cuál fue la modalidad – online, en vivo, online gravado, presencial?)

28. Un curso direccionado hacia el avance de esta discusión, ¿de qué debería tratar?

29. ¿Hay algo que no le pregunté y que ud cree que haría sentido preguntarle?

Apéndice 2 - Familias de códigos

I - Códigos sobre acceso excepcional (AE::) para fines de investigación criminal

AE:: Apoyaría

AE:: Banalización de las roturas de sigilo

AE:: Causará evasión del servicio

AE:: Con controles institucionales rigurosos

AE:: Compromete la legalidad de la prueba

AE:: Costo operacional para el proveedor

AE:: Costo “reputacional” para el proveedor

AE:: Innecesario, pues hay otros medios de investigación

AE:: Es necesario confiar en la justicia

AE:: Hiere los principios de Seguridad de la Información y cifrado

AE:: Hiere la seguridad del Estado

AE:: Impacta la confianza en el ecosistema digital

AE:: Importante en nombre de la seguridad

AE:: Indeterminado si apoyaría

AE:: Manifestación de desconocimiento, duda o incertidumbre

AE:: No apoyaría

AE:: No hay evidencia de ganancia

AE:: Necesario defender para valorizar la autoridad pública

AE:: Obligación de colaborar con la justicia

AE:: Obligación de obedecer comando judicial

AE:: Tan o menos grave que los medios actualmente empleados

AE:: Para crímenes específicos

AE:: Riesgo de abuso por la autoridad

AE:: Risco de usurpación por terceros maliciosos

AE:: Riesgo para derechos

AE:: Semejante a la interceptación telefónica

AE:: Último medicamento

AE:: Vulnera a terceros

II - Códigos sobre satisfacción con el ambiente regulatorio (AR::) sobre cifrado

AR:: Brasil está mejor que el exterior

AR:: Crear una institución para determinar patrones

AR:: Cripto está amenazada

AR:: Decisões del STF son buenas

AR:: Desconoce

AR:: Debe haber estandarización para un nivel mayor de seguridad

AR:: Debe haber protección contra backdoor/bloqueo de apps

AR:: Enforcement es frági

AR:: Se reconoce la importancia de la cifrado

AR:: Inexistente

AR:: Neutralidad tecnológica es positiva/importante

AR:: Positivo, debate sobre going dark ha avanzado

AR:: Poco regulado, no abarca mayor parte de los usos

III - Códigos sobre la legitimidad de los bloqueos de Whatsapp en 2015/16 (BW::) y sobre si el Marco Civil de Internet autoriza tal medida (MCI::)

BW:: Atajo investigativo

BW:: Autoriza, si es proporcional

BW:: Bloqueos fueron desproporcionales

BW:: Bloqueos fueron ilegítimos

BW:: Había desconocimiento sobre la tecnología

BW:: Motivado por disputa de fuerzas

BW:: Ha generado daños económicos

BW:: Ignorancia de las empresas

BW:: Inconstitucional

BW:: Ineficaces, pues personas bajaron VPN

BW:: Interpretación equivocada del Marco Civil de Internet

BW:: Justicia brasileña no-competente

BW:: Legítimos, ley tiene que ser cumplida

BW:: Penaliza la herramienta

BW:: Se puede autorizar

BW:: Primero bloqueo no involucró cifrado

MCI:: Autoriza, pues art. 11 habla de “legislación brasileña”

MCI:: Fuera del poder general de cautela

MCI:: Independiente de MCI, debido al poder general de cautela

MCI:: Independiente de MCI, pues fundamento fue CPP

MCI:: No autoriza

MCI:: No autoriza, pues medida es por demás gravosa

MCI:: No autoriza, pues es prueba diabólica

MCI:: Sanciones son solo para proteger la privacidad

MCI:: Sanciones tienen que existir como recurso final

MCI:: Se recusó a responder

IV - Códigos sobre los conocidos métodos alternativos (MA::) de acceso a informaciones criptografadas y sus riesgos

MA Riesgos:: Incidente de seguridad

MA Riesgos:: Otros

MA Riesgos:: Riesgo de abuso por la autoridad

MA Riesgos:: Violación indiscriminada de la intimidad

MA Riesgos:: Vulnera a terceiros

MA:: Back up

MA:: Búsqueda, aprensión y desbloqueo

MA:: Client-side scanning

MA:: Búsqueda exhaustiva de llave

MA:: Desconoce o no se acuerda

MA:: Ingeniería social

MA:: Espejado del número

MA:: Ghosting

MA:: Infiltración tradicional

MA:: Lawful hacking

MA:: Metadatos

MA:: Otros

MA:: Phishing

MA:: Spyware