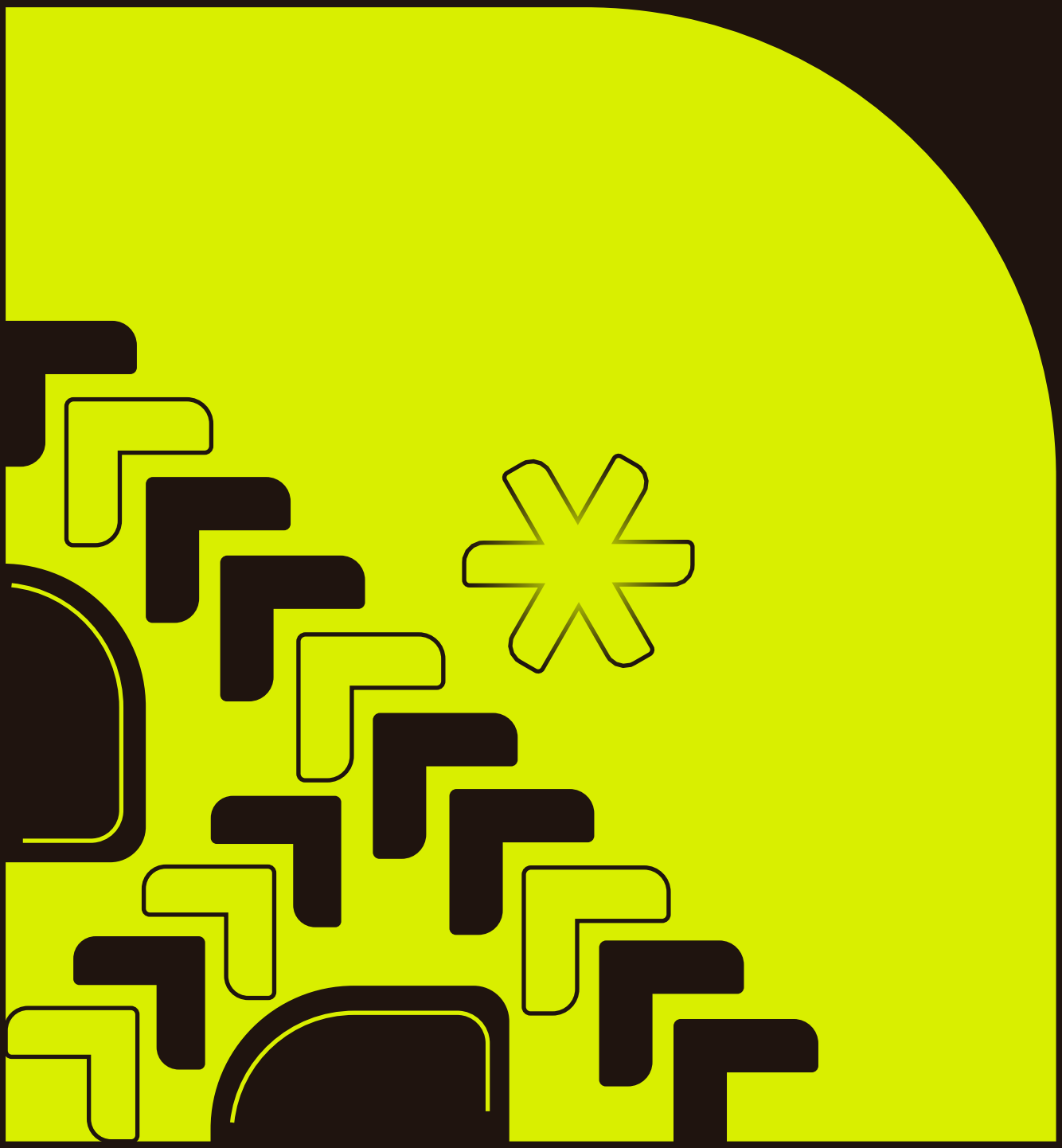
Nota Técnica

Instituto de Pesquisa em Direito & Tecnologia do Recife

Desafíos regulatorios y directrices sobre el uso de herramientas de intrusión digital en el contexto brasileño



FICHA TÉCNICA

Realización:

Instituto de Investigación en Derecho y Tecnología de Recife - IP.rec

Equipo:

Coordinación:

Mariana Canto

Autores:

Mariana Canto
Marcos César M. Pereira
Luana Batista

Revisión:

Raquel Saraiva

Proyecto Gráfico:

Estúdio Puya!

Traducción al español realizada por:

Maria Luana Valois

Cómo citar:

IP.REC - INSTITUTO DE INVESTIGACIÓN EN DERECHO Y TECNOLOGÍA DE RECIFE. Nota Técnica: Desafíos regulatorios y directrices sobre el uso de herramientas de intrusión digital en el contexto brasileño. Recife: IP.rec, 2024.

Nota Técnica: Desafíos Regulatorios Y Directrices Sobre El Uso De Herramientas De Intrusión Digital En El Contexto Brasileño

1. INTRODUCCIÓN

1.1 Contextualización y Objetivos de la Nota Técnica

La presencia de vulnerabilidades en dispositivos y sistemas informáticos es algo extremadamente común en la vida cotidiana, aunque para la mayoría de la población sea algo invisible o desconocido. Estas fallas crean brechas que permiten a atacantes acceder a información que debería estar protegida por capas de seguridad digital. En ocasiones, la explotación de estas vulnerabilidades se lleva a cabo por parte del Estado, sea con fines de inteligencia o de investigación, una práctica denominada *hacking governamental*[1].

El descubrimiento y la explotación de vulnerabilidades por parte del Estado[2] puede llevarse a cabo mediante el propio poder de inteligencia estata[l3] o puede ser externalizado a empresas especializadas en el ámbito de la vigilancia. De esta manera, se crea un mercado con empresas que fomentan la inseguridad cibernética a partir de la venta de exploración de vulnerabilidades a gobiernos y empresas que desarrollan herramientas de intrusión en dispositivos informáticos[4].

Lo que se ha observado, considerando este panorama, fue el aumento de denuncias relacionadas con el abuso e infracciones a los derechos humanos derivadas del uso de herramientas de acceso y extracción de datos de dispositivos móviles. Entre una gama de soluciones, destacó en el escenario internacional el spyware (software espía) Pegasus,

---

[1] DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Hacking Governamental**: uma revisão sistemática. Belo Horizonte: Instituto de Referência em Internet e Sociedade, fevereiro de 2023. Disponible en <https://bit.ly/3YdVcIL>. Acceso en 02 de diciembre de 2024

[2] La práctica también es conocida en la literatura como *lawful hacking*. Cf. BELLOVIN, Steven M. et al. Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. **Nw. J. Tech. & Intell. Prop.**, v. 12, p. 1, 2014. LIGUORI, Carlos. Exploring Lawful Hacking as a Possible Answer to the'Going Dark'Debate. **Mich. Tech. L. Rev.**, v. 26, p. 317, 2019.

[3] Por ejemplo, el *Vulnerabilities Equities Process* es un proceso del gobierno de los Estados Unidos para decidir si una vulnerabilidad descubierta será divulgada para mejorar la seguridad cibernética o si será utilizada de forma ofensiva con fines de inteligencia. Cf. https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF. Acceso en 02 de diciembre de 2024.

[4] Cf. AMARAL, Pedro; CANTO, Mariana; PEREIRA, César M.; RAMIRO, André (coord.). Nutrindo o Mercado de Vulnerabilidades. In: . Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponible en https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da- inseguranca.pdf. Acceso en 02 de diciembre de 2024.

desarrollado por la empresa israelí NSO Group[5]. Capaz de infectar dispositivos y acceder a toda la información sin que el vigilado tenga conocimiento, su utilización fue observada contra activistas, periodistas y disidentes políticos en países como México[6], España[7], Índia[8], Bahrein[9], entre otros. Considerando este escenario, esta nota técnica tiene como objetivo proporcionar insumos para la elaboración de posibles políticas públicas sobre tecnologías de acceso y extracción de datos de dispositivos móviles. Buscaremos presentar aquí, todavía, la relevancia actual del tema, los diversos tipos de herramientas utilizadas, el contexto regulatorio, buenas prácticas y los desafíos en esta temática.

1.2. Relevancia del Tema en el Escenario Actual

Brasil no está distante de esta temática. En el estudio realizado por el IP.rec en 2022, titulado "**Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil**"[10], se identificaron 209 contratos entre el poder público y empresas privadas vendedoras de herramientas de intrusión que atacan dispositivos informáticos. Los datos señalaron la capilaridad de tales soluciones tanto a nivel federal como a nivel estatal, lo que complica las medidas legales y de salvaguarda para el uso de estas soluciones.

El uso de estas herramientas y el tratamiento de los datos recopilados a partir de su operacionalización están marcados por una opacidad generalizada. La ausencia de una Ley General de Protección de Datos (LGPD) en el ámbito penal y de la seguridad nacional genera vacíos que permiten la formulación de políticas públicas preocupantes en relación con los

[5] MARCZAK, Bill et al. HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. Citizen Lab, 2018. Disponible en https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in- -45-countries/. Acceso en 02 de diciembre de 2024

[6] Kirchgaessner, Stephanie. Mexico: reporters and activists hacked with NSO spyware despite assurances. **The Guardian**, 04 de outubro de 2024. Disponible en https://www.theguardian.com/world/2022/oct/04/mexico-nso-spyware-journalists-human-rights-hacked- pegasus Acceso en 02 de diciembre de 2024.

[7] Spain: Court reopens investigation in Pegasus spying scandal. **DW**, 23 de abril de 2024. Disponible en https://www.dw.com/en/spain-court-reopens-investigation-in-pegasus-spying-scandal/a-68901546 Acceso en 02 de diciembre de 2024.

[8] India still targeting high-profile journalists with Pegasus software. **Le Monde**, 28 de diciembre de 2023. Disponible en https://www.lemonde.fr/en/international/article/2023/12/28/india-still-targeting-high-profile-journalists-with-pegasus-software_6382201_4.html Acceso en 02 de diciembre de 2024.

[9] Bahrain: Devices of three activists hacked with Pegasus spyware. **Amnesty International,** 18 de febrero de 2022. Disponible en https://www.amnesty.org/en/latest/news/2022/02/bahrain-devices-of-three-activists-hacked-with-pegasus-spyware/ Acceso en 02 de diciembre de 2024.

[10] AMARAL, Pedro; CANTO, Mariana; PEREIRA, César M.; RAMIRO, André (coord.). Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil [livro eletrônico]. Recife (PE): IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponible en https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf. Acceso en 02 de diciembre de 2024.

derechos fundamentales de los brasileños. Un ejemplo claro en este ámbito es el Proyecto Excel, de la Secretaría de Operaciones Integradas (SEOPI), que depende del Ministerio de Justicia y Seguridad Pública. Creado durante el gobierno del expresidente Jair Bolsonaro, dicho proyecto consistía en el suministro de dispositivos para extraer datos de teléfonos móviles a las secretarías de seguridad pública, a cambio de los datos recopilados durante las operaciones en las que se utilizaron estos recursos[11].

Más recientemente, el uso ilegal por parte de funcionarios de la Agência Brasileira de Inteligência (ABIN) de la solución FirstMile[12],desarrollada por Verint Systems/Cognyte, durante el gobierno de Bolsonaro, fue el centro de atención de los medios de comunicación en Brasil. Este equipo tiene la capacidad de rastrear la ubicación de un objetivo a través de redes 2G, 3G y 4G. Para ello, la herramienta explota vulnerabilidades en las redes de telecomunicaciones, simulando una antena para obtener la ubicación del objetivo[13]. Entre las personas espiadas por la llamada "ABIN paralela" se encontraban ministros del Supremo Tribunal Federal (STF), parlamentarios del Congreso Federal, miembros del Poder Ejecutivo y periodistas[14].

Como resultado de este hecho político, la Procuradoria Geral da República (PGR) presentó una demanda ante el STF cuestionando la falta de regulación en el uso de herramientas de monitoreo remoto. La Acción Directa de Inconstitucionalidad por Omisión (ADO) 84, posteriormente convertida en la Argüición de Incumplimiento de Precepto Fundamental (ADPF) 1143, bajo la ponencia del ministro Cristiano Zanin, tuvo una audiencia pública los días 11 y 12 de junio de 2024.

En el marco de este caso, el Proyecto de Ley 402/2024[15], de autoría del senador Alessandro

[11] Ameno, Fernando. As Planilhas de Bolsonaro: Ministério da Justiça equipa polícias para vasculhar celulares em troca de dados. **The Intercept Brasil,** Rio de Janeiro, 21 de março de 2022. Disponible en: https://www.intercept.com.br/2022/03/21/ministerio-da-justica-equipa-policias-para-vasculhar-celulares- em-troca-de-dados/ . Acceso en 02 de diciembre de 2024.

[12] CNN. FirstMile: como funciona o software espião que teria sido usado pela Abin de Ramagem. **CNN Brasil.** 25 de janeiro de 2024. Disponible en https://www.cnnbrasil.com.br/politica/firstmile-como-funciona-o-software-espiao-que-teria-sido-usado-pela-abin-de-ramagem/ . Acceso em 02 de diciembre de 2024.

[13] Camporez, Patrick, Serra, Paola. 'Abin paralela': PF e Anatel explicam vulnerabilidade que permitiu acesso a localização de celulares. **O Globo,** Rio de Janeiro, 18 de julho de 2024. Disponible en https://oglobo.globo.com/politica/noticia/2024/07/18/abin-paralela-pf-e-anatel-explicam-vulnerabilidade- que-permitiu-acesso-a-localizacao-de-celulares.ghtml. Acceso en 02 de diciembre de 2024.

[14] Sales, Pedro. Lira, Renan Calheiros, Kim Kataguiri: conheça os alvos da Abin paralela. **Congresso em Foco**, 11 de julho de 2024. Disponible en https://congressoemfoco.uol.com.br/area/justica/abin-paralela-arthur-lira-renan-calheiros-kim-kataguiri/. Acceso en 02 de diciembre de 2024.

[15] https://www25.senado.leg.br/web/atividade/materias/-/materia/162146

Vieira (MDB/SE), fue presentado en el Senado Federal. Dicho proyecto regula el uso de herramientas de monitoreo remoto por parte de organismos y agentes públicos, tanto civiles como militares. Este escenario resalta la urgencia de debatir el tema en Brasil, que actualmente carece de una regulación adecuada en la materia, dejando espacio para abusos y violaciones a los derechos humanos.

2. Tecnologías de Acceso y Extracción de Datos en Dispositivos Móviles

2.1. Definición y Tipos de Tecnologías Utilizadas

Durante la investigación de los 'Mercaderes de la Inseguridad', realizamos una división analítica para separar diferentes tipos de herramientas de extracción de datos de dispositivos móviles.

Tipo	Descripción	Ejemplos
Acceso remoto	Soluciones en las que el operador accede al dispositivo del usuario sin necesidad de tener la posesión física del aparato. A partir de la infección del objetivo, el espía tendrá diversas informaciones, dependiendo del nivel de intrusividad del dispositivo.	Pegasus (NSO Group); FirstMile, GI2 e PI2 (Verint Systems/Cognyte)
Acceso con dispositivos en mano	Dispositivos en los que el operador necesita tener la posesión física del aparato para ejecutar la extracción de datos. La extracción se realiza	UFED (Cellebrite); XRY (MSAB); Magnet AXIOM (OpenText); Forensic Toolkit (Exterro/AccessData)

mediante la conexión del dispositivo con la herramienta, que recupera los datos almacenados y/o eliminados del aparato.

Tal distinción es importante para comprender tanto los límites técnicos de su funcionamiento como el contexto de aplicación de cada una. Las primeras poseen un potencial intrusivo significativamente mayor, operando de forma remota y, con frecuencia, infectando el dispositivo sin el conocimiento del usuario. Pegasus, por ejemplo, es capaz de infectar el dispositivo explotando vulnerabilidades en aplicaciones o en el sistema operativo. Estas fallas, cuando incluso los propios fabricantes las desconocen, se denominan vulnerabilidades de día cero[16].

Las últimas, por su parte, requieren la posesión del aparato físico en manos para la extracción de datos, lo que disminuye el poder de intrusividad, pero sigue siendo igualmente preocupante. A pesar de esta diferencia, aún son capaces de recolectar datos de forma extensiva. Al ser utilizadas sobre todo en investigaciones criminales como dispositivos forenses, la alta capacidad de extracción de datos puede capturar información que excede el alcance investigativo, ya sea en el tema y/o en el tiempo del hecho que está siendo investigado, recuperando datos eliminados y generando margen para la fishing expedition (término que hace referencia a la búsqueda exploratoria e indiscriminada de evidencias). Esto ocurre porque tales dispositivos operan mediante la extracción de datos de tres formas:

Forma de extracción	Descripción	Datos obtenidos
Lógica	Método más rápido en el que se crean copias de los archivos accesibles al usuario.	Datos básicos del dispositivo: contactos, historial de llamadas, mensajes de texto, datos de aplicaciones, medios y documentos accesibles.

[16] Pegg, David; Cutler, Sam. What is Pegasus spyware and how does it hack phones. **The Guardian**, 18 de julho de 2021. Disponible en https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones . Acceso en 03 de diciembre de 2024

Sistema de archivos (file system)	Proceso aún considerado lógico, pero más amplio, que accede y copia toda la estructura del sistema de archivos del dispositivo, recuperando incluso archivos ocultos y metadatos del sistema.	Todos los datos de la extracción lógica, además de los archivos del sistema, cachés de aplicaciones, archivos temporales, registros del sistema y archivos ocultos.
Física	Método más complejo y completo, en el que se extrae una copia bit a bit de la memoria de almacenamiento del usuario, permitiendo la recuperación de datos eliminados. Requiere más tiempo y recursos técnicos.	Todos los datos de las extracciones anteriores, además de archivos eliminados y fragmentos de datos no asignados.

Fuente: Producción propia a partir del informe del Privacy International (2019)[17]

En nuestro estudio identificamos una presencia extendida de soluciones de intrusión digital que requieren el acceso físico a los dispositivos en los órganos de seguridad pública estatales. Los dispositivos de intrusión remota identificados se encontraban, en su mayoría, en organismos federales, como el Ministerio de Defensa. A nivel estatal, estas herramientas fueron contratadas en menor número, sin que fuera posible identificar un patrón en las motivaciones para su adquisición.

2.1. Riesgos Potenciales Asociados a los Derechos Fundamentales y Libertades Civiles

Cada una de estas herramientas trae consigo riesgos para los derechos humanos, especialmente en escenarios con pocas salvaguardas. Como se destacó anteriormente, las soluciones de intrusión digital han estado involucradas en numerosos casos de violaciones a los derechos humanos. Además del caso Pegasus, el más conocido, las herramientas desarrolladas por las empresas Verint Systems/Cognyte y Cellebrite también han estado implicadas en

[17] Privacy International. **A technical look at Phone Extraction.** 2019. Disponible en https://privacyinternational.org/sites/default/files/2019-10/A%20technical%20look%20at%20Phone%20Extraction%20FINAL.pdf . Acceso en 02 de diciembre de 2024.

escándalos de violaciones a los derechos humanos y han sido adquiridas en gran medida por el Estado brasileño.

A nivel internacional, las soluciones de Cognyte fueron utilizadas para interceptar y vigilar las comunicaciones de ciudadanos de Sudán del Sur. Durante dos años, la empresa recibió más de 760 mil dólares por estos equipos[18]. En Myanmar, la misma empresa ganó un proceso de licitación antes del golpe militar de febrero de 2021, en el cual se emplearon sus soluciones para interceptar las telecomunicaciones[19].

En Brasil, además del caso FirstMile, las soluciones de Verint/Cognyte fueron utilizadas en una investigación de la Policía Civil de Pará sobre el gobernador del estado, Helder Barbalho (MDB/PA). Durante la operación, los equipos fueron detenidos bajo la sospecha de haber sido utilizados de manera irregular para monitorear a los investigadores de un esquema de corrupción en la administración pública[20].

Aunque desarrolla soluciones de intrusión con acceso físico a los dispositivos, Cellebrite también está involucrada en escándalos similares. La herramienta de la empresa, también israelí, estuvo vinculada a la persecución de periodistas en Myanmar[21]. Otros países en los que se tiene registro del uso de esta solución para la extracción de datos de periodistas, activistas y opositores políticos incluyen Botsuana, Ghana, Nigeria, Hong Kong, Bangladesh, Indonesia, India, Rusia, Bielorrusia, Venezuela, Bahréin y Arabia Saudita[22].

En Estados Unidos, la organización UpTurn identificó que la solución UFED, desarrollada por Cellebrite[23], estaba extendida, presente en todos los estados del país. Sin embargo, su uso había trascendido el ámbito de los delitos de mayor potencial ofensivo, siendo utilizada en crímenes

---

[18] Kabir, Omer. Verint Systems supplied South Sudan with surveillance technology says Amnesty. **Calcalist**, 02 de fevereiro de 2021. Disponible en https://www.calcalistech.com/ctech/articles/0,7340,L-3891006,00.html . Acceso en 03 de diciembre de 2024.

[19] Potkin, Fanny; Mcpherson, Poppy. Israel's Cognyte won tender to sell intercept spyware to Myanmar before coup-documents. **Reuters**. 23 de janeiro de 2023. Disponible en https://www.reuters.com/technology/israels-cognyte-won-tender-sell-intercept-spyware-myanmar-before- coup-documents-2023-01-15/ . Acceso en 04 de diciembre de 2024.

[20] O Antagonista. A empresa que vendeu a 'maleta hacker' para o esquema de Helder Barbalho. **O Antagonista,** 02 de outubro de 2020. Disponible en https://oantagonista.com.br/brasil/exclusivo-a-empresa-que-vendeu-a-maleta-hacker-para-o-esquema-de-helder-barbalho/ . Acceso en 03 de diciembre de 2024.

[21] McLaughin, Tommy. Security-tech companies once flocked to Myanmar. One firms tools were used against two journalists. **The Washington Post**, 4 de maio de 2019. Disponible en https://www.washingtonpost.com/world/asia_pacific/security-tech-companies-once-flocked-to-myanmar-one-firms-tools-were-used-against-two-journalists-/2019/05/04/d4e9f7f0-5b5d-11e9-b8e3-b03311fbbbfe_story.html . Acceso en 04 de diciembre de 2024.

[22] Krapiva, Natália; Hinako. What spy firm Cellebrite can't hide from investors. **AccessNow**, 26 de maio de 2021. Disponible en https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/ Acceso en 04 de diciembre de 2024.

[23] Koepke, Logan et al. **Mass Extraction**. UpTurn, 2020. Disponible en https://www.upturn.org/work/mass-extraction/ . Acceso en 04 de diciembre de 2024.

como grafiti, hurto, prostitución, accidentes de tráfico y delitos relacionados con drogas ilegales. Debido a este uso, el estudio indica una alta probabilidad de que las extracciones hayan afectado de manera desproporcionada a personas negras y latinas.

Tal inferencia también es posible en el escenario brasileño. El Proyecto Excel, mencionado anteriormente en la nota técnica, distribuía dispositivos de Cellebrite a las secretarías de seguridad pública estatales. En un video promocional publicado por el Ministerio de Justicia y Seguridad Pública, el delito más investigado fue el de tráfico de drogas, representando el 66% de los delitos investigados. Según datos del Instituto de Pesquisa Econômica Aplicada (IPEA), las personas negras son la mayoría de los detenidos por tráfico de drogas en rondas policiales[24]. De este modo, es muy probable que los datos enviados a las bases de datos del Proyecto Excel presenten un sesgo racial, lo que constituye un riesgo para las políticas de seguridad pública que se desarrollen a partir del análisis de dicha información.

Estos abusos señalan los riesgos asociados a la producción y el uso de estas herramientas. La existencia de las mismas implica la creación y el mantenimiento de vulnerabilidades que ponen en riesgo los datos y la información de diversos sectores de la sociedad. Este hecho dificulta el mantenimiento de un ecosistema digital seguro y estable para todos, por lo que es necesario tener en cuenta esta situación en el desarrollo de cualquier política nacional de ciberseguridad.

Además, estas soluciones de intrusión en dispositivos representan una grave amenaza para los derechos humanos. Como se presentó, tales herramientas están siendo empleadas para la persecución de activistas, periodistas, disidentes políticos y minorías sociales. Así, más allá del derecho a la privacidad, derechos como la libertad de expresión, de prensa, de asociación e incluso el derecho a la vida pueden verse amenazados por herramientas como estas. Tal amenaza no solo proviene del uso de estas soluciones contra objetivos específicos, sino también de la capacidad de su existencia para inhibir a los ciudadanos de manifestarse libremente por miedo a la vigilancia y represión estatal, lo que provoca el "efecto de enfriamiento" (*chilling effect)*.

Es importante señalar también que, una vez adquiridas estas herramientas, el arsenal intrusivo estará disponible tanto para gobiernos democráticos como autoritarios. De la misma manera, una vez dentro del marco estatal, sin las debidas regulaciones, salvaguardas y transparencia, existe una alta probabilidad de que estas soluciones sufran un secuestro de función (*function creep)*.

Por último, pero no menos importante, la expansión de las soluciones de intrusión dentro del ámbito policial brasileño genera preocupaciones, especialmente en las ciudades con alta presencia de milicias. Por ello, es necesario tener en cuenta la posibilidad de que herramientas

[24] G1. Negros são maioria entre presos por tráfico de drogas em rondas policiais, diz IPEA. **G1**, 13 de março de 2024. Disponible en https://g1.globo.com/politica/noticia/2024/03/13/negros-sao-maioria-entre-presos-por-trafico-de-drogas-em-rondas-policiais-diz-ipea.ghtml . Acceso en 05 de diciembre de 2024.

de intrusión estén siendo utilizadas para extraer datos de ciudadanos en áreas controladas por milicias como una forma de control y vigilancia del territorio, lo que pone en un mayor riesgo a las personas ya socialmente vulnerables.

3. Contexto Legal y Regulatorio

3.1. Escenario Brasileño Actual

3.1.1. Constitución Federal de Brasil

Además del derecho a la privacidad garantizado por el artículo 5º, inciso X, de la Constitución, que juega un papel central en el análisis de los derechos que pueden ser limitados mediante el uso de herramientas de acceso y extracción de datos, el acceso a la información de las comunicaciones privadas también está protegido por el inciso XII del mismo artículo. Cualquier acción para acceder a información privada, incluidas las comunicaciones, debe realizarse mediante procedimientos legales que aseguren su legalidad, proporcionalidad y justificación de necesidad. Además, la necesidad de una autorización judicial adecuadamente fundamentada es esencial.

La Enmienda Constitucional nº 115/2022 incorporó al artículo 5º (inciso LXXIX) de la Constitución brasileña el derecho fundamental e independiente a la protección de datos personales. Es decir, las normas infraconstitucionales y los instrumentos administrativos que regulan el uso de herramientas de acceso y extracción deben tener siempre en cuenta la protección de los derechos fundamentales consagrados en la Constitución. La observancia de principios como finalidad, necesidad, calidad de los datos, transparencia, seguridad, prevención y responsabilidad de los responsables del tratamiento de los datos en las operaciones de acceso y extracción debe basarse en el derecho constitucional a la protección de los datos personales.

Es importante destacar que la protección de estos derechos va más allá del ámbito individual, afectando, especialmente cuando se trata de la recopilación de datos a gran escala, a servicios como los correos electrónicos, las redes sociales, las aplicaciones de mensajería instantánea y los navegadores, afectando a comunidades enteras cuyos datos son recopilados. Por lo tanto, las pruebas de proporcionalidad y necesidad en el uso de estas herramientas deben considerar el impacto sobre los derechos de otros individuos, que a menudo no están involucrados en una investigación criminal, pero verán sus derechos suspendidos debido a las rutinas investigativas y de vigilancia de esta naturaleza.

3.1.2. Marco Civil de Internet (MCI)

El MCI establece que es necesaria una orden judicial para la custodia y el acceso a los registros de conexión, aplicaciones y contenidos de las comunicaciones (Art. 7º, II y III; Art. 10, §§1º y 2º; Art. 15, §1º). Es decir, al aplicar el MCI, existe un procedimiento legal que debe seguir la entidad responsable de la investigación cuando el acceso a los datos y las comunicaciones sea

intermediado por un proveedor de servicios, ya sea de conexión o de aplicación. Sin embargo, cuando el acceso se realiza directamente al dispositivo, sin la participación de un intermediario, el MCI no establece directrices claras ni específicas, lo que puede generar espacio para arbitrariedades, inseguridad jurídica y abusos en la vigilancia. En cualquier acción de recopilación, almacenamiento, custodia y procesamiento de registros, datos personales o comunicaciones por parte de proveedores de conexión y aplicaciones de internet, cuando al menos uno de estos actos ocurra en Brasil, el MCI impone la obligación de seguir la legislación brasileña, garantizando el derecho a la privacidad, la protección de los datos personales, así como el secreto de las comunicaciones privadas y los registros.

3.1.1. Ley General de Protección de Datos (LGPD) y LGPD Penal

Aunque la Ley General de Protección de Datos (LGPD) establece normas sobre el uso de datos personales en el sector público y privado, el artículo 4º de la LGPD excluye de su alcance el tratamiento de datos realizado con 'fines de seguridad pública, defensa nacional, seguridad del Estado e investigación y represión de infracciones penales' (inciso III, letras 'a' a 'd').Al igual que el Reglamento General de Protección de Datos de la Unión Europea (GDPR), la legislación brasileña prevé excepciones en el ámbito de la seguridad pública. Sin embargo, a diferencia de la regulación europea, que creó una directiva específica para tratar el ámbito penal (Directiva 2016/680), Brasil aún no dispone de una legislación propia que aborde este tema.

3.1.2. PL 402/2024

El Proyecto de Ley Nº 402/2024, presentado por el Senador Alessandro Vieira (MDB/SE), tiene como objetivo regular el uso de herramientas de monitoreo remoto de terminales de comunicaciones personales por parte de organismos y agentes públicos, tanto civiles como militares.

Uno de los aspectos principales del PL es el énfasis en la observancia de principios fundamentales como la legalidad, proporcionalidad, necesidad, seguridad, transparencia y supervisión, alineados con los establecidos en la Ley General de Protección de Datos (LGPD).Además, el PL asegura que la utilización de estas herramientas estará condicionada a una autorización judicial previa, lo que refuerza la necesidad de protección contra posibles abusos.

Cabe destacar la amplitud del PL, que no solo regula la extracción de datos de dispositivos individuales, sino también la recopilación masiva de datos, una cuestión cada vez más relevante debido a la evolución de las tecnologías de vigilancia a gran escala.

Otro punto crucial del PL es la criminalización del monitoreo sin orden judicial, además de la obligación de informar sobre incidentes relacionados con fallas o abusos en el uso de estas herramientas.Estas disposiciones constituyen un paso importante en la construcción de un marco legal robusto, destinado a asegurar la responsabilidad de los agentes públicos involucrados y prevenir abusos de poder. Sin embargo, el proyecto no menciona los posibles

remedios legales disponibles para las víctimas de vigilancia arbitraria.

Aunque el proyecto presenta avances importantes, también requiere un mayor debate sobre las prácticas de vigilancia y supervisión, con participación multisectorial. Es importante considerar la inclusión de más detalles sobre la elaboración de informes circunstanciados para aumentar la transparencia del proceso. También es esencial incluir medidas que garanticen el debido proceso legal, con el fin de prevenir la violación de la cadena de custodia, ya que estas herramientas pueden alterar el contenido de los dispositivos infectados.

Finalmente, el proyecto no incluye una disposición que impida al Estado establecer relaciones comerciales con empresas involucradas en violaciones de derechos humanos, tanto nacionales como internacionales. La creación de una lista de empresas que cumplan con estos criterios, junto con la prohibición de hacer negocios estatales con estas entidades, reforzaría el compromiso de Brasil con los derechos fundamentales y la soberanía nacional.

Es importante destacar que, aunque el PL representa una excelente oportunidad para debatir en profundidad este tema, no suple la necesidad de una LGPD penal, ya que esta ofrecería un marco legal general de protección de datos personales en el ámbito de la seguridad pública, la seguridad nacional y la defensa del Estado, de manera que ambas propuestas serían complementarias, no excluyentes.

En resumen, el Proyecto de Ley Nº 402/2024 representa un avance importante en la regulación de las prácticas de vigilancia en Brasil, proponiendo un modelo legal que busca equilibrar los derechos a la privacidad con la necesidad de seguridad pública. Si se implementa adecuadamente, el PL podría posicionar a Brasil como líder mundial en la protección de los derechos digitales, inspirando legislaciones similares en otros países, tal como ocurrió con el Marco Civil de Internet.

3.1.3. Acción de Descumplimiento de Precepto Fundamental 1143

La Acción de Descumplimiento de Precepto Fundamental (ADPF) 1143 trata del cuestionamiento realizado por la Procuraduría General de la República (PGR) sobre la falta de regulación del uso de softwares de monitoreo por parte de los organismos públicos. Inicialmente, este tema llegó al Supremo Tribunal Federal (STF) a través de la Acción Directa de Inconstitucionalidad por Omisión (ADO) 84, en la cual la PGR criticó la ausencia de una acción normativa del Congreso Nacional para regular el uso de estas tecnologías. La PGR argumentó que estas herramientas han sido empleadas por los órganos de inteligencia y represión del Estado para realizar vigilancia remota e invasiva de dispositivos móviles, bajo el pretexto de combatir el terrorismo y el crimen organizado. Posteriormente, la acción fue convertida en ADPF 1143 a solicitud de la propia Procuraduría General de la República.

A principios de 2024, el Ministro Cristiano Zanin, relator del caso, solicitó información al Congreso Nacional y envió los autos a la Abogacía General de la Unión (AGU) y a la PGR. En abril del mismo año, el Ministro determinó la realización de una audiencia pública con el objetivo de reunir información técnica y empírica sobre el tema, la cual fue programada para

los días 10 y 11 de junio. El Instituto de Protección de Derechos de las Comunicaciones (IP.rec) participó en dicha audiencia y presentó una serie de contribuciones relevantes a la discusión.

En mayo de 2024, el Ministro Cristiano Zanin ordenó que los Tribunales de Cuentas de la Unión, de los estados y de los municipios proporcionarán información sobre la existencia de procesos administrativos relacionados con licitaciones, adquisiciones o contrataciones de spyware para dispositivos de comunicación personal, como teléfonos móviles y tabletas. En cuanto a los programas de rastreo, el Ministro aclaró que las herramientas en cuestión incluyen, pero no se limitan a, Pegasus, Imsi Catchers (como el Pixcell y el G12), así como aplicaciones que monitorean la ubicación de objetivos específicos, como el First Mile y el Landmark. Hasta noviembre de 2024, más de 20 Tribunales de Cuentas enviaron documentos a la corte[25].

3.2. Legislación Internacional Relevante

3.2.1. Legislaciones e Iniciativas

a) Iniciativas Estadunidenses

En 2021, el Departamento de Comercio de los Estados Unidos anunció la inclusión de empresas de spyware en su "Entity List", una lista que agrupa a individuos, empresas y organizaciones extranjeras consideradas una amenaza para la seguridad nacional de los Estados Unidos. Esta inclusión implica restricciones de exportación y requisitos de licencia para determinadas tecnologías y productos. Ese mismo año, las empresas israelíes NSO Group y Candiru fueron añadidas a la lista[26]. En 2023, la lista se amplió con la inclusión de las empresas Intellexa, con sede en Grecia e Irlanda, y Cytrox AD, con sede en Hungría y Macedonia del Norte[27].

En 2024, la empresa canadiense Sandvine también fue añadida a la lista después de que sus productos fueran utilizados para la vigilancia masiva en la web, la censura y ataques contra activistas de derechos humanos y disidentes, incluido el uso indebido de software espía comercial. No obstante, en octubre de 2024, la empresa fue retirada de la lista tras implementar una serie de medidas para abordar el uso indebido de su tecnología. Estas medidas incluyeron una reestructuración corporativa, cambios en el liderazgo y en el modelo de negocio, con un enfoque en atender a democracias comprometidas con la protección de los

[25] https://portal.stf.jus.br/processos/detalhe.asp?incidente=690081
[26] U.S. Department of Commerce. Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities. 2021. Disponible en https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list Acceso en 10 de diciembre de 2024
[27] U.S. Department of State. The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities. 2023. Disponible en https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities-2/ Acceso en 10 de diciembre de 2024

derechos humanos. Además, Sandvine se comprometió a salir de países no democráticos, habiendo abandonado ya 32 y estando en proceso de salida de otros 24. El gobierno de Estados Unidos también destacó el "fortalecimiento de relaciones con la sociedad civil", la "asignación de ganancias para la protección de los derechos", la "inclusión de expertos en derechos humanos en el nuevo equipo de liderazgo", la "evaluación de las decisiones comerciales a través del recién creado Comité de Ética Empresarial" y el "monitoreo riguroso del uso indebido de la tecnología en los países donde la empresa pretende permanecer"[28].

En marzo de 2023, durante la segunda Cúpula por la Democracia organizada por Estados Unidos, 11 países firmaron una declaración conjunta reconociendo la amenaza representada por el uso indebido de spyware comercial. Los firmantes destacaron la necesidad urgente de establecer controles rigurosos, tanto nacionales como internacionales, para contener la proliferación de estas herramientas. Posteriormente, la declaración fue actualizada para incluir nuevos países que se unieron al compromiso multilateral de combatir el uso abusivo de estas tecnologías. En marzo de 2024, durante la tercera Cúpula por la Democracia, países como Finlandia, Alemania, Japón, Polonia, Irlanda y Corea del Sur reafirmaron su apoyo a medidas concretas para enfrentar los riesgos asociados al uso de spyware comercial[29].

La declaración enfatiza que el spyware comercial ha sido utilizado indebidamente tanto por regímenes autoritarios como por democracias, a menudo para perseguir a opositores políticos, intimidar a disidentes, suprimir la libertad de expresión y violar derechos humanos. En respuesta, los países firmantes se comprometieron a adoptar medidas rigurosas para garantizar que el uso de spyware por parte de sus gobiernos sea coherente con los derechos humanos, el estado de derecho y las libertades civiles. Además, los países se comprometieron a implementar prácticas sólidas de control de exportaciones, impidiendo el envío de tecnologías a usuarios que puedan utilizarlas para "actividades maliciosas".

Sin embargo, la experiencia práctica ha demostrado que, en muchas ocasiones, estos controles son fácilmente eludidos o no se aplican con suficiente rigor, como han señalado investigaciones realizadas por miembros del Parlamento Europeo[30]. Aunque el compromiso con una mayor cooperación internacional y el intercambio de información sobre el uso indebido de spyware es positivo, aún faltan mecanismos claros y efectivos para garantizar que estas medidas tengan un

---

[28] Bureau of Industry and Security. Commerce Removes Sandvine from Entity List Following Significant Corporate Reforms to Protect Human Rights. 2024. Disponible en https://www.bis.gov/press-release/commerce-removes-sandvine-entity-list-following-significant-corporate-reforms-protect Acceso en 10 de diciembre de 2024

[29] The White House. Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware. **The White House.** 2024. Disponible en https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/18/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/ Acceso en 10 de diciembre de 2024

[30] Sophie in 't Veld. European Parliament Draft Recommendation to the Council and the Commission pursuant to Rule 208(12) of the Rules of Procedure following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware. **European Parliament**. Disponible en https://www.europarl.europa.eu/doceo/document/PEGA-RD-740554_EN.pdf Acceso em 10 de diciembre de 2024

impacto real en la contención de la proliferación de esta tecnología.

En resumen, aunque la declaración de marzo de 2023 representa un avance en el reconocimiento del problema, las acciones concretas hasta el momento no reflejan la magnitud de la amenaza. Es probable que la administración de Trump no continúe con la campaña del gobierno de Biden para limitar la proliferación de tecnologías de spyware comercial, ampliamente utilizadas por regímenes autoritarios para perseguir a periodistas, activistas de derechos civiles y opositores políticos. Trump y sus aliados mantienen estrechas relaciones políticas y financieras con dos de los mayores consumidores de estas herramientas, Arabia Saudita y Emiratos Árabes Unidos, lo que demuestra una postura negligente frente a las violaciones de derechos humanos cometidas por estos regímenes.
Según Steven Feldstein, del Carnegie Endowment for International Peace, es muy probable que haya retrocesos en las políticas de control del software espía, ya que la administración de Trump priorizaría los argumentos de contraterrorismo presentados por las empresas de spyware en detrimento de las críticas de los defensores de los derechos digitales[31]. En este contexto, empresas como NSO Group, que mantienen vínculos estrechos con el gobierno israelí alineado con Trump, probablemente encontrarán un entorno más favorable para sus operaciones.

Medios de comunicación informaron que, hasta octubre de 2024, NSO había gastado más de 1,8 millones de dólares en actividades de lobby, según documentos del Foreign Agents Registration *Act*[32]. La empresa ha centrado sus esfuerzos en establecer conexiones con legisladores republicanos y ha intentado aprovechar el contexto de la guerra de Israel para aumentar sus posibilidades de reanudar sus actividades. Además, se ha promocionado como voluntaria en la guerra de Gaza, afirmando que ayuda a localizar israelíes desaparecidos y rehenes. Este intento de convencer al gobierno estadounidense de permitir su regreso ha sido visto como una estrategia de "lavado de imagen" por parte de NSO.

a) Pall Mall Process

En febrero de 2024, los gobiernos del Reino Unido y de Francia lanzaron, en Londres, el Pall Mall Process (PMP), una iniciativa orientada al diálogo sobre la "proliferación y el uso irresponsable de capacidades comerciales de intrusión cibernética"[33]. La declaración resultante

[31] Eric Geller. More Spyware, Fewer Rules: What Trump's Return Means for US Cybersecurity. **Wired**. 14 de novembro de 2024. Disponible en https://www.wired.com/story/trump-administration-cybersecurity-policy-reversals/ Acceso em 10 de diciembre de 2024.
[32] Georgia Gee. Pegasus spyware maker said to flout federal court as it lobbies to get off U.S. blacklist. **The Intercept**. 21 de outubro de 2024. Disponible en https://theintercept.com/2024/10/21/pegasus-spyware- nso-israel-lobbying-republicans/ Acceso em 10 de diciembre de 2024.
[33] Foreign, Commonwealth and Development Office. The Pall Mall Process declaration: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities. 2024. **UK government.** Disponible en https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process - tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities Acceso en 10 de diciembre de 2024.

del evento inicial subrayó principios orientadores como la responsabilidad (*accountability)*, la precisión, la supervisión y la transparencia, destacando la importancia de las asociaciones público-privadas y de la colaboración multisectorial, además de expresar preocupaciones sobre la seguridad nacional, los derechos humanos y las libertades fundamentales.

Sin embargo, surgen algunas cuestiones críticas en el contexto de esta iniciativa. La limitada participación de países fuera del eje del Norte Global es un aspecto relevante, ya que la falta de diversidad geopolítica puede comprometer la eficacia del diálogo y la representatividad de las voces globales en el debate sobre ciberseguridad. Además, el proceso de discusiones, realizado a puerta cerrada y sin la presencia de medios de comunicación, plantea interrogantes sobre la transparencia y la inclusión de diferentes actores y perspectivas. Esta falta de visibilidad puede restringir el impacto del evento y disminuir la confianza pública en la integridad del proceso.

Otro punto a tener en cuenta es la ausencia de países que son grandes productores de herramientas de intrusión cibernética, como Israel, así como de empresas proveedoras de esos recursos. La ausencia de estos actores centrales puede dificultar la implementación efectiva de los principios establecidos, dado que la gobernanza internacional sobre el uso de tales tecnologías depende, en gran medida, del compromiso de las partes involucradas en la producción y comercialización de esas herramientas.

Finalmente, la limitada participación de organizaciones de la sociedad civil representa una laguna significativa en un proceso que pretende ser multisectorial. Estas organizaciones desempeñan un papel crucial en iluminar un mercado de ciberseguridad opaco y, por lo tanto, su inclusión en discusiones de esta índole es esencial para garantizar la transparencia y la equidad en las decisiones que afectan los derechos digitales y la seguridad global.

En resumen, aunque el PMP presenta un avance importante en el abordaje de cuestiones críticas relacionadas con la ciberseguridad, su eficacia futura dependerá de la ampliación de la participación internacional, de una mayor transparencia en el proceso y de la inclusión activa de todos los sectores involucrados, incluidos los actores globales y las organizaciones de la sociedad civil.

3.1.1. Precedentes

Aunque los casos judiciales puedan basarse en información filtrada o en análisis forenses digitales que identifiquen señales características del uso de herramientas de intrusión, la falta de un registro integral, accesible, confiable y completo de las operaciones realizadas con estas tecnologías por parte de los gobiernos dificulta tanto para las víctimas la comprobación de los hechos de sus alegaciones como para las autoridades judiciales la realización de investigaciones adecuadas sobre todas las circunstancias. El número de solicitudes aprobadas presentadas por aquellos afectados por el uso ilegal de herramientas digitales (tanto víctimas individuales como empresas de tecnología cuyos sistemas fueron invadidos ilegalmente) sigue siendo limitado en la jurisdicción brasileña. Sin embargo, en los últimos años, ha aumentado la cantidad de fallos directamente relacionados con el uso de estas herramientas para monitorear y perseguir a periodistas y defensores de los derechos humanos, especialmente en diversos tribunales

regionales de protección de los derechos humanos.

En marzo de 2024, en una decisión histórica en el caso Miembros del Colectivo de Abogados José Alvear Restrepo (CAJAR) v. Colombia, la Corte Interamericana de Derechos Humanos identificó una violación del derecho a la privacidad y enfatizó las tensiones que el desarrollo tecnológico y la circulación generalizada de datos traen al ámbito de la protección de los derechos humanos[34], destacando, por lo tanto, la importancia de la autorización judicial, de la supervisión independiente de las actividades de inteligencia y de la necesidad de soluciones eficaces.

La decisión también determinó que las operaciones de inteligencia – que en este caso involucraron el uso de spyware y malware, entre otras tecnologías – solo son legales y válidas cuando están acompañadas de controles sólidos y medidas de salvaguarda. Ecoando su fallo anterior en Escher et al. vs Brasil[35], la Corte enfatizó que proteger la privacidad y la libertad de expresión es fundamental, y que cualquier medida de vigilancia debe ser autorizada por una autoridad judicial que defina su alcance, duración y límites.

Ya en el continente europeo, en el caso Pietrzak y Bychawska-Siniarska y otros v. Polonia, en mayo de 2024, el Tribunal Europeo de Derechos Humanos (TEDH) concluyó por unanimidad que la ley de vigilancia de Polonia de 2016 violaba el artículo 8.º de la Convención Europea de Derechos Humanos, que protege el derecho a la privacidad[36]. El Tribunal identificó tres cuestiones clave en la ley, particularmente relacionadas con el uso de spyware comercial como el Pegasus: (i) la falta de salvaguardias adecuadas, como la ausencia de exigencia de autorización judicial y recursos; (ii) la retención excesivamente amplia de datos de comunicación; y (iii) la supervisión inadecuada.

Aún en Europa, en los casos *Liberty y otros v. Reino Unido, Roman Zakharov v. Rusia y Pietrzak* y *Bychawska-Siniarska y otros v. Polonia*, la falta de supervisión eficaz y de soluciones disponibles bajo la legislación nacional para aquellos sujetos a herramientas secretas de vigilancia digital, como el spyware por agencias estatales, fue considerada una violación del Artículo 13 de la Convención Europea de Derechos Humanos, es decir, el derecho a un recurso efectivo en casos de violación de derechos humanos.

---

[34] CORTE INTERAMERICANA DE DIREITOS HUMANOS. Miembros de la Corporación Colectivo de Abogados “José Alvear Restrepo” v. Colômbia. Sentença de 18 de outubro de 2023. Corte Interamericana de Direitos Humanos. Disponible en https://privacyinternational.org/sites/default/files/2024-03/seriec_506_esp.pdf . Acceso en 10 diciembre 2024.

[35] CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso Escher e outros Vs. Brasil. Sentença de 6 de julho de 2009. Sentença de 20 de novembro de 2009. Disponible en https://www.corteidh.or.cr/docs/casos/articulos/seriec_208_por.pdf Acceso en 10 de diciembre de 2024.

[36] TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Pietrzak v. Poland and Bychawska-Siniarska and others v. Poland. Disponible en https://hudoc.echr.coe.int/eng#{"itemid":["002-14333 Acceso en 10 diciembre 2024.

4. Buenas Prácticas y Directrices para la Adquisición y Uso de Tecnologías por parte del Gobierno Federal

4.1. Soberanía Nacional y Procedencia de las Tecnologías Adquiridas

Como observó el Comité de Investigación del Parlamento Europeo, que investiga el uso de Pegasus y de spyware de vigilancia equivalente, los países del Norte Global son vistos como lugares atractivos para las sedes de empresas de tecnología y servicios de vigilancia[37].

De acuerdo con estudios recientes, grandes proveedoras de herramientas de intrusión digital, como Cellebrite, FinFisher, Blue Coat, Hacking Team, Nexa Technologies, CyberPoint, L3 Technologies, Verint, Sandvine y NSO Group, están ubicadas en países considerados democráticos, como Estados Unidos, Italia, Francia, Alemania, Canadá e Israel[38]. A pesar de ello, muchas de estas empresas han suministrado tecnologías tanto para regímenes autocráticos como para el uso ilegítimo por gobiernos democráticos alrededor del mundo.

Desde 2022, sin embargo, se observa un cambio en el discurso de diferentes gobiernos respecto a la necesidad de desarrollar un marco regulatorio que busque frenar la proliferación y la amenaza representada por el "uso indebido" de herramientas de intrusión digital. En este sentido, creemos que Brasil necesita implementar un control más riguroso sobre la importación de estas herramientas, con el fin de evitar que sean desarrolladas por o adquiridas de actores que violen o contribuyan a la violación de derechos humanos, o que pongan en riesgo su soberanía nacional.

Considerando los evidentes riesgos para los derechos humanos y las dificultades de supervisión, el ex-Relator Especial de la ONU sobre la libertad de expresión, David Kaye, propuso una moratoria sobre el comercio de tecnologías de vigilancia, con el objetivo de "permitir que los Estados desarrollen un régimen de control y exportación y mejoren los marcos legales que protejan la privacidad"[39]. Esta solicitud fue respaldada por varios responsables de mandatos de Procedimientos Especiales de la ONU. En 2022, Costa Rica se convirtió en el primer país en solicitar la implementación de esta moratoria[40]. Así, es esencial

[37] Sophie in 't Veld. European Parliament Draft Recommendation to the Council and the Commission pursuant to Rule 208(12) of the Rules of Procedure following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware. **European Parliament**. Disponible en https://www.europarl.europa.eu/doceo/document/PEGA-RD-740554_EN.pdf Acceso en 10 de diciembre de 2024.

[38] Steven Fieldstein. Governments Are Using Spyware on Citizens. Can They Be Stopped? **Carnegie Endowment.** 2021. Disponible en https://carnegieendowment.org/posts/2021/07/governments-are-using-spyware-on-citizens-can-they-be-stopped?lang=en Acceso en 10 de diciembre de 2024.

[39] United Nations. UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools. Disponible en https://www.ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance Acceso en 10 de diciembre de 2024.

[40] Access Now. Stop Pegasus: Costa Rica is the first country to call for a moratorium on spyware technology. 2022. Disponible en https://www.accessnow.org/press-release/costa-rica-first-country-moratorium- spyware Acceso en 10 de diciembre de 2024.

que el gobierno brasileño considere la posibilidad de una moratoria en la compra de ciertos equipos de vigilancia privada con mayor capacidad intrusiva, hasta que se establezcan reglas claras y responsables. Esta medida está justificada por la gravedad de los daños causados por estas tecnologías.

Finalmente, es importante observar los avances en otras jurisdicciones. Empresas como Meta y Apple ya han demandado a proveedores de herramientas de intrusión, como el NSO Group, debido al uso de softwares como Pegasus contra sus usuarios[41]. El grupo israelí argumentó que, dado que sus productos son utilizados por gobiernos extranjeros y agencias de aplicación de la ley, estaría protegido por inmunidad soberana en territorio estadounidense. Sin embargo, el Tribunal de Apelaciones del 9º Circuito rechazó esta alegación, creando un precedente importante para la responsabilización de las empresas de spyware[42]. La decisión permitió la apertura de un proceso legal contra la empresa, siendo un hito relevante para la discusión sobre la responsabilidad en el uso de estas tecnologías.

4.2 Garantías de Transparencia y Mecanismos de Monitoreo y Auditoría

Evidencias, como las presentadas en nuestro estudio **"Mercadores da Insegurança: Conjuntura e Riscos do Hacking Governamental no Brasil"**, hacen imperativo que el gobierno brasileño sea transparente respecto a sus esfuerzos para garantizar que los servicios de investigación y seguridad nacional operen en conformidad con los derechos fundamentales y las libertades civiles. Durante la recolección de datos realizada por investigadores de IP.rec para nuestro estudio, a partir de portales de transparencia y solicitudes fundamentadas por la Ley de Acceso a la Información, se constató que el nivel de transparencia respecto a la adquisición de estas herramientas por organismos públicos sigue siendo considerado bajo.

Además, organismos responsables por el escrutinio y la supervisión, como la ANPD y tribunales de cuentas, no deberían enfrentar dificultades para obtener esta información. La supervisión independiente sobre los servicios de inteligencia y la adquisición de herramientas de intrusión en Brasil es notoriamente débil y, en muchos casos, inexistente. Es fundamental que los mecanismos de investigación *ex-ante* y *ex-post* sean fortalecidos. La creación de un mecanismo de supervisión independiente para el uso de estas tecnologías es urgente y necesaria. Medidas como estas han establecido formas más eficaces de proteger los derechos y las libertades civiles de la población.

---

[41] Stephanie Kirchgaessner. Court orders maker of Pegasus spyware to hand over code to WhatsApp. **The Guardian**. 29 de fevereiro de 2024. Disponible en https://www.theguardian.com/technology/2024/feb/29/pegasus-surveillance-code-whatsapp-meta-lawsuit-nso-group Acceso em 10 de diciembre de 2024.

[42] UCI Law. One step closer to holding NSO Group accountable: The U.S. Solicitor General recommended the Supreme Court deny NSO's cert petition concerning the applicability of foreign sovereign immunity to a private entity. Disponible en https://ijclinic.law.uci.edu/2022/11/22/one-step-closer-to-holding-nso-group-accountable-the-u-s-solicitor-general-recommended-the-supreme-court-deny-nsos-cert-petition-concerning-the-applicability-of-foreign-sovereign-immunity-t/ Acceso en 10 de diciembre de 2024.

Es imprescindible que el gobierno brasileño asegure que las alegaciones de monitoreo ilegal y abuso de herramientas de intrusión sean investigadas adecuadamente y que los responsables sean sancionados cuando sea necesario. También deben establecerse reglas claras para limitar el uso de la "seguridad nacional" como justificación para la vigilancia, garantizando una supervisión judicial apropiada y el respeto a las libertades y garantías fundamentales.

Cabe también destacar que las herramientas de intrusión digital no están aisladas en este escenario, sino que forman parte de toda una red de instituciones y actores. El uso de estas herramientas a menudo depende de la (in)existencia de medidas regulatorias, salvaguardias legales y mecanismos de supervisión. Como observó el Parlamento Europeo, muchas veces, de forma intencional o no, los sistemas regulatorios han sido distorsionados, total o parcialmente, o diseñados de manera que faciliten el uso de mecanismos altamente intrusivos de monitoreo[43]. Así, el uso ilegítimo o abusivo de estas herramientas deja de ser un incidente y se convierte en una estrategia. Por lo tanto, se recomienda que el gobierno brasileño base el uso de estas herramientas requiere un soporte legal preciso y específico, con mecanismos de supervisión robustos.

También deben existir recursos legales que sean eficaces frente a la obstrucción por parte de los órganos gubernamentales. Como observó Ní Aoláin, los Estados a menudo establecen sistemas judiciales separados, como "tribunales secretos", para manejar casos de seguridad nacional[44]. Las actividades de vigilancia realizadas por las agencias estatales dificultan los mecanismos tradicionales de responsabilidad. Además, la transferencia transnacional de tecnología impone desafíos jurisdiccionales y prácticos específicos. El gobierno brasileño no debe permitir que la participación de entidades privadas en el desarrollo y operación de estas herramientas de intrusión haga aún más difícil el acceso a recursos eficaces para abordar violaciones de derechos.

4.3 Capacitación y Especialización de las Autoridades Responsables

El derecho a un juicio justo es un elemento crucial del Estado Democrático de Derecho. Los Estados garantizan este derecho no sólo asegurando la independencia de los jueces y tribunales, sino también preservando la integridad de las evidencias digitales y garantizando que tanto la acusación como la defensa tengan acceso igualitario a la información relevante, incluidos los datos sobre la cadena de custodia.
La capacitación y especialización de las autoridades responsables de la administración de

[43] Sophie in 't Veld. European Parliament Draft Recommendation to the Council and the Commission pursuant to Rule 208(12) of the Rules of Procedure following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware. **European Parliament**. Disponible en https://www.europarl.europa.eu/doceo/document/PEGA-RD-740554_EN.pdf Acceso en 10 de diciembre de 2024.
[44] Fionnuala Ní Aoláin. United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. **United Nations.** Abril de 2023. Disponible en https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf

justicia y la protección de los derechos fundamentales son elementos esenciales para garantizar la preservación de la integridad del proceso judicial, especialmente en un contexto en el que las evidencias digitales juegan un papel central. El caso Rook v. Alemania, analizado por el Tribunal Europeo de Derechos Humanos, ejemplifica los desafíos que surgen debido al uso de tecnologías digitales en los procesos judiciales, al destacar la violación del derecho a un juicio justo derivada de fallas en la preservación y el acceso a las evidencias digitales, incluida la cadena de custodia[45]. La integridad de estas evidencias es fundamental para asegurar que los derechos de la defensa sean respetados y que las pruebas puedan ser impugnadas de manera significativa, tal como enfatizó el Tribunal.

La cuestión de la protección de datos y la preservación de las evidencias digitales también fue resaltada por el ex Relator Especial de la ONU sobre la libertad de expresión, David Kaye, quien alertó sobre los riesgos de adulteración de los registros digitales a través del uso de herramientas como los spyware[46]. Ciertas herramientas de intrusión digital, al permitir la alteración discreta de datos sin dejar rastros, representan una grave amenaza para la imparcialidad del proceso judicial y el derecho a un juicio justo, ya que pueden ser utilizadas tanto por actores estatales como por otros agentes, para modificar información de manera intencional o accidental. El uso de tales herramientas, por lo tanto, exige una regulación rigurosa y la formación específica de los agentes involucrados, con el fin de mitigar los riesgos de manipulación de evidencias.

La evolución de las tecnologías de vigilancia, como Pegasus, requiere una adaptación en el marco regulatorio global. La presión por un sistema legal más robusto busca reconocer que ciertas herramientas de intrusión, debido a sus características inherentes, no deben ser utilizadas en procesos judiciales, ya que su capacidad para alterar datos sin dejar rastros compromete el principio de integridad de las evidencias[47]. El Supervisor Europeo de Protección de Datos destacó que la vigilancia digital intensificada y las herramientas asociadas, al cambiar la dinámica de investigación y juicio, requieren de autoridades altamente calificadas que puedan asegurar el uso legítimo de estas tecnologías dentro de los límites del Estado de Derecho[48].

Por lo tanto, la formación técnica y la especialización de las autoridades brasileñas responsables de la recolección, preservación y análisis de evidencias digitales son fundamentales para garantizar que el proceso judicial no se vea comprometido por el uso indebido de estas herramientas. Además, la colaboración internacional entre Brasil y diferentes

---

[45] TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Rook v. Germany. 25 de julho de 2019. Disponible en https://hudoc.echr.coe.int/eng#{"itemid":["001-194614"]}. Acceso en 10 de diciembre de 2024.

[46] David Kaye e Sarah McKune. The Scourge of Commercial Spyware—and How to Stop It. **Lawfare**. 2023. Disponible en https://www.lawfaremedia.org/article/the-scourge-of-commercial-spyware-and-how-to-stop-it Acceso en 10 de diciembre de 2024.

[47] Fionnuala Ní Aoláin. United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. **United Nations.** Abril de 2023. Disponible en https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf Acceso em 10 de diciembre de 2024.

jurisdicciones, con el objetivo de intercambiar conocimientos y buenas prácticas, resulta esencial para que las autoridades puedan responder de manera eficaz a los desafíos que plantea la vigilancia digital y la integridad de las evidencias, preservando así los derechos humanos y el Estado Democrático de Derecho[48].

4.4 Participación de la Sociedad Civil y Especialistas en el Tema

En los últimos años, la participación activa de la sociedad civil ha sido esencial para resaltar las implicaciones éticas y los abusos relacionados con el uso de herramientas de intrusión digital. Organizaciones no gubernamentales, periodistas y activistas han sido los principales responsables de exponer el uso indebido de estas tecnologías, especialmente en regímenes autoritarios o en contextos de vigilancia indiscriminada en democracias. Sin embargo, a pesar de su contribución crucial para visibilizar el problema, la sociedad civil sigue siendo marginalizada en las discusiones sobre la regulación y la responsabilización de estos actos, a menudo en detrimento de un enfoque más técnico y transparente.

La falta de una participación efectiva de la sociedad civil y de expertos en la materia compromete el proceso de formulación de políticas públicas destinadas a la protección de derechos fundamentales, como la privacidad y la libertad de expresión. Especialistas en tecnología, derechos humanos y seguridad digital han advertido sobre la necesidad de crear un entorno regulatorio más inclusivo y participativo, donde se puedan escuchar diversas voces. De este modo, la participación de la sociedad civil y de los expertos es esencial para garantizar un equilibrio entre la seguridad y la libertad, además de asegurar que las normas adoptadas estén alineadas con los principios democráticos y los derechos humanos.

La contribución de expertos en áreas como los derechos digitales es crucial para asegurar que la regulación del uso de herramientas de intrusión digital esté fundamentada en un conocimiento técnico robusto y en un enfoque centrado en los derechos fundamentales. En Brasil, un debate interdisciplinario y transparente es esencial para que el proceso de formulación de políticas públicas no esté dominado exclusivamente por intereses económicos o de seguridad, sino que también considere los impactos sociales e individuales del uso de estas tecnologías.

La creación de un entorno regulatorio inclusivo y participativo asegura que las normas adoptadas estén alineadas con los principios democráticos y los derechos humanos, evitando abusos y excesos en el uso de herramientas de intrusión digital, que pueden ser fácilmente mal utilizadas para fines de vigilancia indiscriminada, como se ha evidenciado en los trabajos del IP.rec, periodistas y otros representantes de la sociedad civil. La colaboración entre la sociedad civil y las autoridades públicas es, por lo tanto, esencial para construir un sistema de control

[48] European Data Protection Supervisor. EDPS Preliminary Remarks on Modern Spyware. 2022. Disponible en https://www.edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en Acceso en 10 de diciembre de 2024.

más justo y eficaz sobre el uso de estas tecnologías en Brasil.

5. Desafíos y Consideraciones Finales

El constante desafío de equilibrar la protección de los ciudadanos con los derechos humanos garantizados es crucial. A menudo, el Estado utiliza la narrativa de protección para introducir equipos de intrusión y vigilancia, cuando en realidad estos representan más riesgos e inseguridad.

El desarrollo tecnológico de soluciones digitales genera fallos técnicos. Aunque no intencionalmente, el surgimiento de nuevas vulnerabilidades crea mayores áreas de ataque para actores malintencionados. A menudo, estas fallas son desconocidas por los equipos de desarrollo, que solo se enteran de ellas mucho después. Como resultado, las empresas de intrusión y los programas de recompensas por vulnerabilidades (bug bounties) explotan comercialmente estas fallas, mientras que los Estados las utilizan para fines de inteligencia.

En este sentido, es necesario avanzar en ciberseguridad, un campo que progresa constantemente en la investigación de nuevas técnicas de protección, ofreciendo niveles superiores de seguridad. Sin embargo, por otro lado, las soluciones de intrusión también avanzan, desarrollando y descubriendo nuevas formas de eludir mecanismos de defensa, generando un ciclo continuo de inseguridad que parece crecer cada vez más.

Es por ello que, frente al rápido desarrollo tecnológico, es necesario actualizar constantemente las políticas de ciberseguridad y regular las herramientas de intrusión digital. Todos los incrementos deben tener en cuenta esta situación para crear un entorno más seguro para los usuarios.

Ante estos desafíos y avances tecnológicos, es fundamental que Brasil adopte un enfoque proactivo para proteger a sus ciudadanos, promoviendo la transparencia en las operaciones de vigilancia y asegurando que cualquier uso de herramientas de intrusión digital sea monitoreado adecuadamente. El fortalecimiento de marcos legales, mecanismos de supervisión e inclusión de diversos sectores de la sociedad, incluidos expertos y organizaciones civiles, es crucial para garantizar que el uso de estas tecnologías sea transparente, responsable y alineado con principios democráticos.

En Brasil, es esencial que el gobierno adopte medidas rigurosas para controlar la importación y el uso de estas herramientas, garantizando que no se utilicen para violar derechos fundamentales ni amenazar la soberanía nacional. Además, la capacitación de las autoridades responsables de la investigación y el análisis de evidencias digitales, la transparencia en las adquisiciones de tecnologías de vigilancia y la implementación de un control efectivo sobre su uso son fundamentales para garantizar que los derechos de la población estén protegidos y que el uso de tecnologías digitales esté en conformidad con el Estado Democrático de Derecho

6. Recomendaciones

Promoción de la transparencia en los procesos de licitación: Se recomienda incrementar la transparencia en los procesos de licitación pública con respecto a la adquisición de productos y la contratación de servicios de intrusión digital con empresas del sector privado, observando posibles cuestiones relacionadas con la seguridad pública y nacional, así como con los derechos humanos.

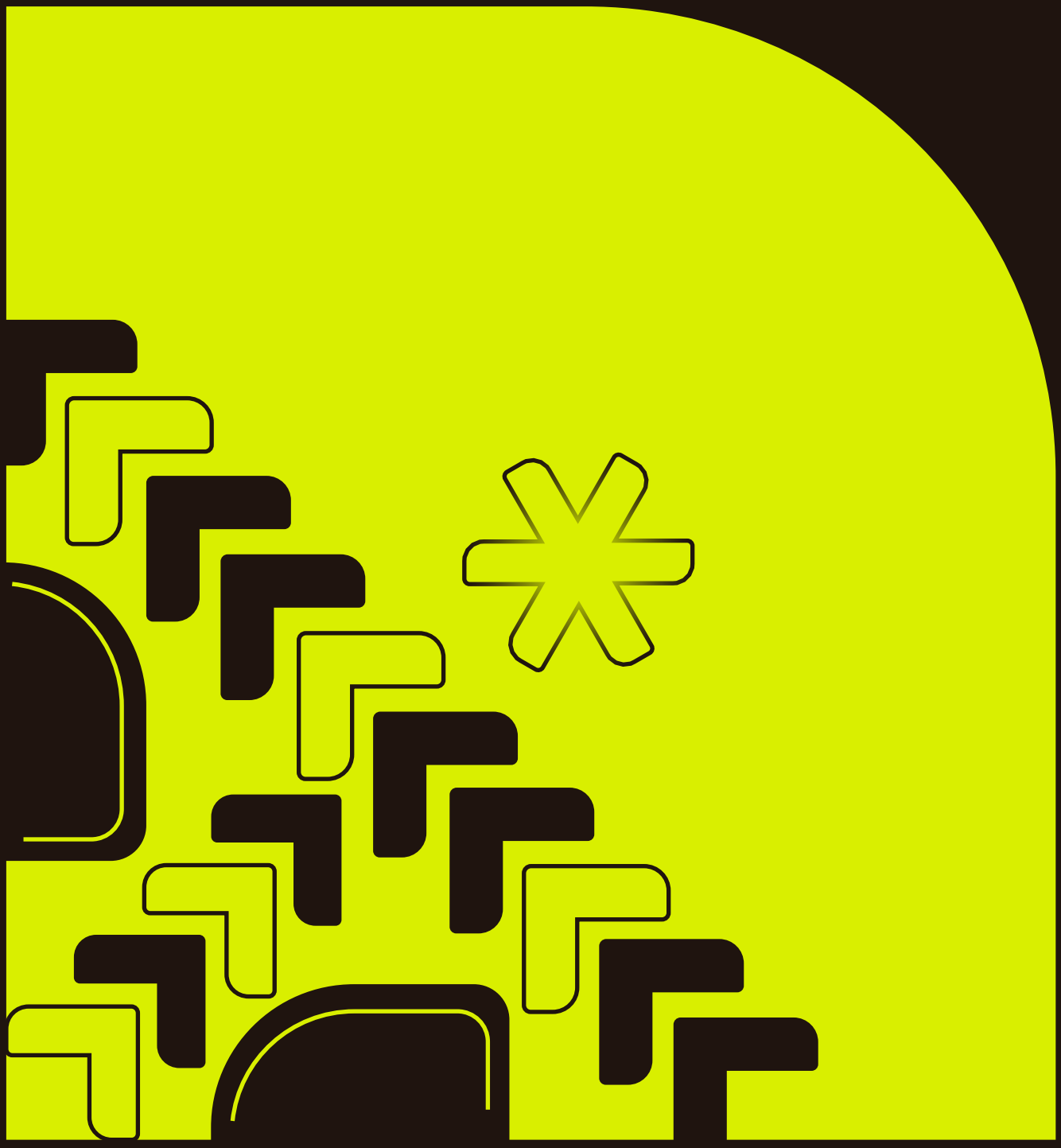
Garantía de transparencia en el uso de herramientas de intrusión digital: Se sugiere que, en caso de utilizar herramientas de intrusión digital, se promueva una total transparencia para garantizar el cumplimiento de las normas legales y éticas, además de preservar la confianza pública y la protección de los derechos fundamentales y las libertades civiles.

Observancia de los derechos humanos por parte de las empresas contratadas: Se aconseja evitar la contratación de empresas implicadas en la vigilancia o recopilación de información sobre activistas, académicos, periodistas, disidentes, figuras políticas o miembros de organizaciones no gubernamentales o comunidades marginadas, con el objetivo de limitar la libertad de expresión o permitir abusos de los derechos humanos o la supresión de las libertades civiles.

Prohibición de herramientas de intrusión sin criterios de confiabilidad: Se propone la prohibición del uso de herramientas de intrusión digital, especialmente las remotas, que no cuenten con características de auditabilidad, transparencia y especificidad, como es el caso de Pegasus.

Implementación de una moratoria sobre herramientas de alta capacidad intrusiva: Se alienta implementar una moratoria sobre el uso y adquisición de herramientas digitales con alta capacidad intrusiva hasta la creación de una regulación adecuada para el tema.

Aprobación de la Ley General de Protección de Datos Penales: Es esencial la aprobación de una Ley General de Protección de Datos para fines de seguridad pública, defensa nacional e inteligencia, con el objetivo de garantizar la protección de la privacidad y los derechos individuales.



Instituto de
Pesquisa em
Direito & Tecnologia
do Recife