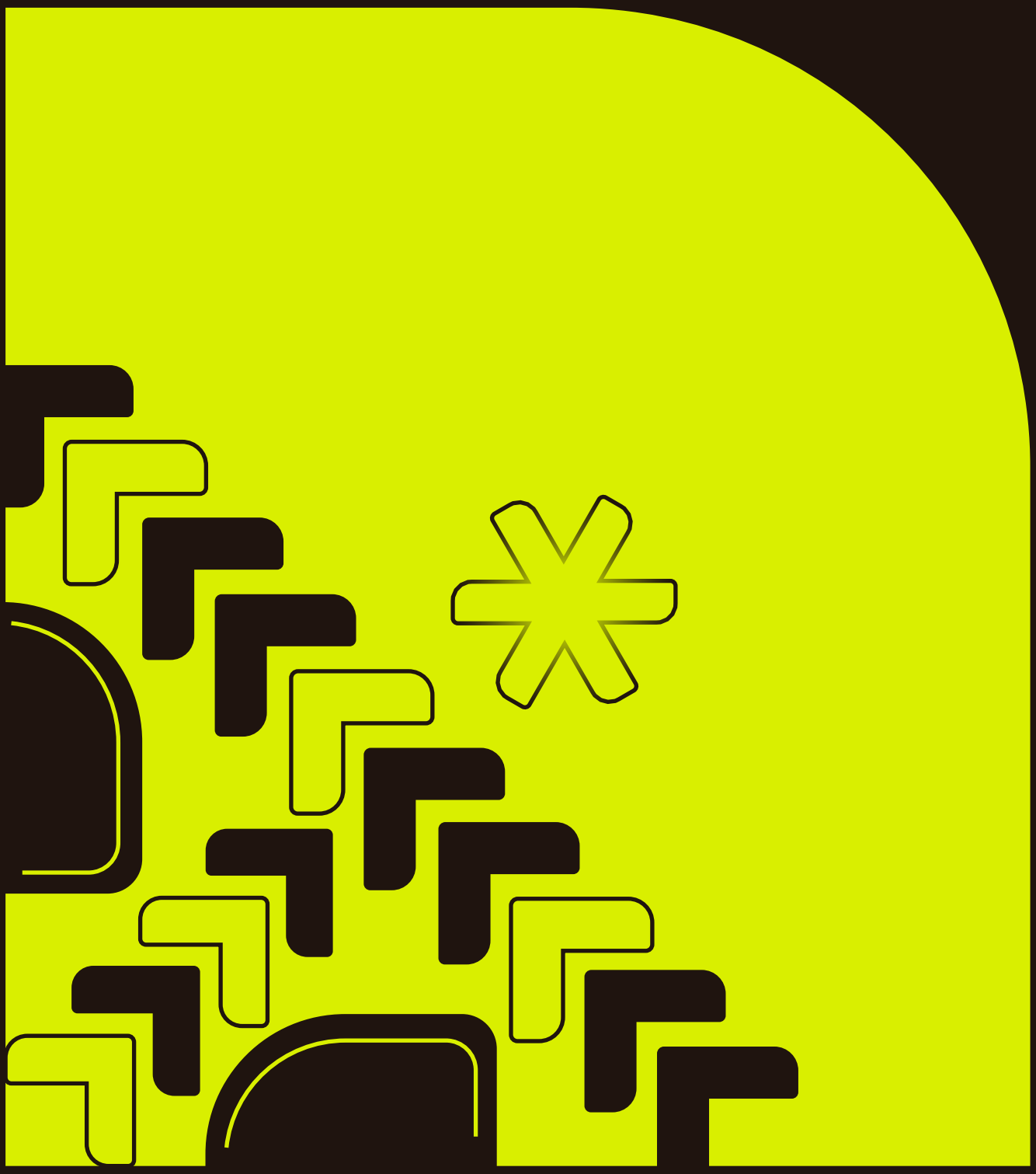
Technical Note

Instituto de Pesquisa em Direito & Tecnologia do Recife

Regulatory challenges and guidelines regarding the use of cyber intrusion tools in the Brazilian context



PUBLICATION DETAILS

Produced by

Produced by Law and Technology Research Institute of Recife - IP.rec

Team:

Coordinator:

Mariana Canto

Authors:

Mariana Canto
Marcos César M. Pereira
Luana Batista

Proofreading:

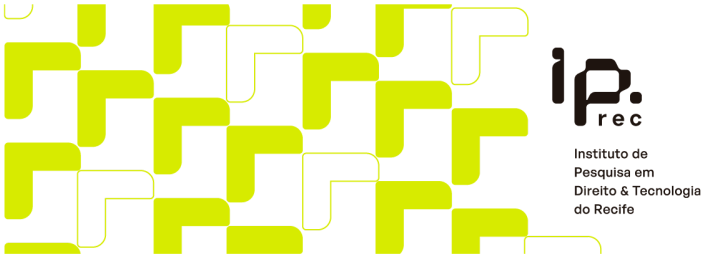
Raquel Saraiva

Graphic Design:

Estúdio Puya!

How to cite:

IP.REC - LAW AND TECHNOLOGY RESEARCH INSTITUTE OF RECIFE. Technical Note: Regulatory challenges and guidelines regarding the use of cyber intrusion tools in the Brazilian context. Recife: IP.rec, 2024.



Technical Note: Regulatory challenges and guidelines regarding the use of digital intrusion tools in the Brazilian context

1. INTRODUCTION

1.1. Context and Objectives of the Technical Note

The presence of vulnerabilities in devices and computer systems is a constant part of daily life, even though for most of the population it remains invisible or unknown. These flaws create openings for attackers to access information that should be protected by layers of digital security. Sometimes, the exploitation of these vulnerabilities is carried out by the state, whether for intelligence or investigative purposes, a practice known as *government hacking*.[1]

The discovery and exploitation of vulnerabilities by the state[2] can be done through the state's own intelligence power[3] or may be outsourced to specialised companies in the surveillance sector. This creates a market where companies foster cybersecurity insecurity to sell exploitation tools to governments and businesses that develop intrusion tools for computer systems.[4]

What was observed within this context was an increase in reports of abuse and human rights violations resulting from the use of tools for accessing and extracting data from mobile devices. Among a range of solutions, the spyware Pegasus, developed by the Israeli company NSO Group,[5] stood out on the international stage. Capable of infecting devices and accessing all information without the target's knowledge, its use was

---

[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, February, 2023. Available at: <https://bit.ly/3YdVcIL>. Accessed on December 2, 2024.

[2] The practice is also known in the literature as 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] For example, the Vulnerabilities Equities Process is a process used by the U.S. government to decide whether a discovered vulnerability will be disclosed to improve cybersecurity or if it will be used offensively for intelligence purposes.

[4] IP.rec. Nourishing the Vulnerability Market." In: _____. "**Merchants of Insecurity: Context and Risks of Government Hacking in Brazil**" [electronic book]. Recife (PE): IP.rec – Institute for Research in Law and Technology of Recife, 2022. Available at: https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf. Accessed on December 2, 2024.

[5] MARCZAK, Bill et al. "HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries." **Citizen Lab**, 2018. Available at: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/. Accessed on December 2, 2024.

observed against activists, journalists, and political dissidents in countries such as Mexico,[6] Spain,[7] India,[8] Bahrain,[9] and others.

Considering this context, the objective of this technical note is to provide input for the development of potential public policies on technologies for accessing and extracting data from mobile devices. We aim to present the relevance of this topic in the current landscape, the various types of tools used, the regulatory context, best practices, and the challenges associated with the issue.

1.2. Relevance of the Topic in the Current Context

Brazil is not distant from this issue. In the study conducted by IP.rec in 2022, titled " Merchants of Insecurity: Context and Risks of Government Hacking in Brazil.,"[10] 209 contracts between the public sector and private companies selling intrusion tools for information devices were identified. The data highlighted the widespread use of such solutions at both the federal and state levels, complicating legal and protective measures for the use of these tools.

The use of these tools and the handling of the data collected through their operation are marked by widespread opacity. The absence of a General Data Protection Law (LGPD) for the criminal and national security spheres opens gaps for the formulation of public policies that raises concerns about the fundamental rights of Brazilians. A clear example in this area is the Project Excel, from the Secretariat of Integrated Operations (SEOPI), linked to the Ministry of Justice and Public Security, created during the government of

---

[6] Kirchgaessner, Stephanie. "Mexico: Reporters and Activists Hacked with NSO Spyware Despite Assurances." **The Guardian**, October 4, 2022. Available at: https://www.theguardian.com/world/2022/oct/04/mexico-nso-spyware-journalists-human-rights-hacked-pegasus. Accessed on December 2, 2024.

[7] Spain: Court reopens investigation in Pegasus spying scandal. **DW**, April 23, 2024. Available at: https://www.dw.com/en/spain-court-reopens-investigation-in-pegasus-spying-scandal/a-68901546 Accessed on December 2, 2024.

[8] India still targeting high-profile journalists with Pegasus software. **Le Monde**, 28 December, 2023. Available at https://www.lemonde.fr/en/international/article/2023/12/28/india-still-targeting-high-profile-journalists-with-pegasus-software_6382201_4.html Accessed on December 2, 2024.

[9] Bahrain: Devices of three activists hacked with Pegasus spyware. **Amnesty International,** 18 February 2022. Available at https://www.amnesty.org/en/latest/news/2022/02/bahrain-devices-of-three-activists-hacked-with-pegasus-spyware/ Accessed on December 2, 2024.

[10] IP.rec. **Merchants of Insecurity: Context and Risks of Government Hacking in Brazil**" [electronic book]. Recife (PE): IP.rec – Institute for Research in Law and Technology of Recife, 2022. Available at: https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf.

former President Jair Bolsonaro. This project involved sending mobile phone data extraction tools to state security secretariats in exchange for the data collected in operations where these tools were used.[11]

More recently, the illegal use by employees of the Brazilian Intelligence Agency (ABIN) of the FirstMile[12] solution, developed by Verint Systems/Cognyte, during the Bolsonaro administration, gained attention in Brazilian news. The equipment has the ability to monitor the location of the target through the use of 2G, 3G, and 4G networks. To achieve this, the tool exploits vulnerabilities in telecommunications networks, simulating a tower to obtain the target's location.[13] Among the individuals spied on by the so-called "parallel ABIN" were Supreme Federal Court (STF) ministers, members of the Federal Congress, executive branch officials, and journalists.[14]

As a result of this political event, the Attorney General's Office (PGR) filed a lawsuit with the STF questioning the lack of regulation regarding the use of remote monitoring tools. The Direct Action of Unconstitutionality for Omission 84, which was transformed into an Argument of Non-Compliance with Fundamental Precept 1143 and reported by Minister Cristiano Zanin. A public hearing regarding the issue took place on June 11 and 12, 2024.

Still in the wake of the case, Bill 402/2024[15] was filed in the Federal Senate, authored by Senator Alessandro Vieira (MDB/SE). The bill addresses the use of remote monitoring tools by public bodies and agents, both civilian and military. This situation underscores the urgency of discussing the topic in Brazil, which currently lacks proper regulation in this area, leaving room for abuses and violations of human rights.

---

[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 March, 2022. Available at: https://www.intercept.com.br/2022/03/21/ministerio-da-justica-equipa-policias-para-vasculhar-celulares-em-troca-de-dados/ . Accessed on December 2, 2024.

[12] CNN. FirstMile: como funciona o software espião que teria sido usado pela Abin de Ramagem. **CNN Brasil.** 25 January, 2024. Available at: https://www.cnnbrasil.com.br/politica/firstmile-como-funciona-o-software-espiao-que-teria-sido-usado-pela-abin-de-ramagem/ . Accessed on December 2, 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 July, 2024. Available at: https://oglobo.globo.com/politica/noticia/2024/07/18/abin-paralela-pf-e-anatel-explicam-vulnerabilidade-que-permitiu-acesso-a-localizacao-de-celulares.ghtml. Accessed on December 2,2024.

[14] Sales, Pedro. Lira, Renan Calheiros, Kim Kataguiri: conheça os alvos da Abin paralela. **Congresso em Foco**, 11 July, 2024. Available at: https://congressoemfoco.uol.com.br/area/justica/abin-paralela-arthur-lira-renan-calheiros-kim-kataguiri/. Accessed on December 2,2024.

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

2. On Tools for Accessing and Extracting Data from Mobile Devices

2.1. Definition and Types of Technologies Used

During the "Merchants of Insecurity" research, we conducted an analytical division to categorise different types of tools for extracting data from mobile devices.

Access method	Description	Example
Remote access	Solutions that allow the operator to access the user's device without needing physical possession of the device. Once the target is infected, the agent will have access to various types of information, depending on the level of intrusiveness of the device.	Pegasus (NSO Group); FirstMile, GI2 e PI2 (Verint Systems/Cognyte)
Physical access (authorities in possession of the device)	Devices in which the operator needs physical possession of the device to carry out data extraction. The extraction is done by connecting the device to a tool that will retrieve both stored and/or deleted data from the device	UFED (Cellebrite); XRY (MSAB); Magnet AXIOM (OpenText); Forensic Toolkit (Exterro/AccessData)

This distinction is important for understanding both the technical limitations of their operation and the context in which each tool is applied. The first type has considerably higher intrusive potential, operating remotely and often infecting the device without the user's knowledge. Pegasus, for example, is capable of infecting the user's device by

exploiting vulnerabilities in apps or the operating system. These flaws, when unknown to the manufacturers themselves, are referred to as zero-day vulnerabilities.[16]

The second type, in turn, requires physical possession of the device in order to extract data, which reduces their intrusiveness, but remains equally concerning. Despite this difference, they are still capable of collecting data extensively. Primarily used in criminal investigations as forensic devices, their high data extraction capacity can capture information beyond the investigative scope, whether in terms of subject matter or the timeframe of the event being investigated. They can recover deleted data and create opportunities for a "fishing expedition" (a term referring to the indiscriminate, exploratory search for evidence). This occurs because these devices operate by extracting data in three ways:

Method of extraction	Description	Obtained data
Logical	The quickest method, where copies of the files accessible to the user are created.	Basic device data: contacts, call history, text messages, app data, media, and accessible documents.
File system	A process still considered logical, but more comprehensive, that accesses and copies the entire file system structure of the device, including hidden files and system metadata.	All the data from logical extraction, as well as system files, app caches, temporary files, system logs, and hidden files.
Physical	A more complex and comprehensive method, in which a bit-by-bit copy of the user's storage memory is extracted, allowing the recovery of deleted data. It requires more time and technical resources.	All the data from previous extractions, as well as deleted files and unallocated data fragments.

[16] Pegg, David; Cutler, Sam. What is Pegasus spyware and how does it hack phones. **The Guardian**, 18 July, 2021. Available at: https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones . Accessed on 02 December, 2024

Source: Own production based on the Privacy International report (2019)[17]

In our study, we identified the widespread use of digital intrusion solutions in state public security agencies that require physical possession of the devices. The remote intrusion devices identified were, for the most part, within federal agencies, such as the Ministry of Defense. At the state level, such tools were contracted as well, though in smaller numbers, and it was not possible to identify a pattern in the motivations for their acquisition.

2.2. Potential Risks Associated with Fundamental Rights and Civil Liberties

Each of these tools carries risks associated with human rights, especially in contexts with low safeguards. As previously highlighted, digital intrusion solutions have been involved in numerous cases of human rights violations. Beyond the well-known Pegasus case, tools developed by companies like Verint Systems/Cognyte and Cellebrite have also been involved in human rights violations and have been widely acquired by the Brazilian government.

Internationally, Cognyte's solutions were involved in the interception and surveillance of communications of citizens in South Sudan. Over a period of two years, more than 760 thousand dollars were paid to the company for equipment.[18] In Myanmar, the same company won a bidding process before the military coup in February 2021, which was used to intercept telecommunications.[19]

In Brazil, beyond the FirstMile case, Verint/Cognyte solutions were involved in an investigation by the Civil Police of Pará against the state governor, Helder Barbalho (MDB/PA). During the operation, the equipment was seized on suspicion of being used irregularly to monitor investigators working on a corruption scheme within the public administration.[20]

---

[17] Privacy International. **A technical look at Phone Extraction.** 2019. <https://privacyinternational.org/sites/default/files/2019-10/A%20technical%20look%20at%20Phone%20Extraction%20FINAL.pdf> . Accessed on 02 December, 2024

[18] Kabir, Omer. Verint Systems supplied South Sudan with surveillance technology says Amnesty. **Calcalist**, 02 February 2021. Available at https://www.calcalistech.com/ctech/articles/0,7340,L-3891006,00.html . Accessed on 03, December, 2024.

[19] Potkin, Fanny; Mcpherson, Poppy. Israel's Cognyte won tender to sell intercept spyware to Myanmar before coup-documents. **Reuters**. 23 January 2023. Available at: https://www.reuters.com/technology/israels-cognyte-won-tender-sell-intercept-spyware-myanmar-before-coup-documents-2023-01-15/ . Accessed on 04, December 2024.

[20] O Antagonista. A empresa que vendeu a 'maleta hacker' para o esquema de Helder Barbalho. **O Antagonista,** 02 October, 2020. Available at: https://oantagonista.com.br/brasil/exclusivo-a-empresa-que-vendeu-a-maleta-hacker-para-o-esquema-de-helder-barbalho/ . Accessed on 03, December 2024.

Although Cellebrite develops intrusion solutions that require physical possession of devices, the company is also involved in similar scandals. The company's tool, also Israeli-made, has been linked to the persecution of journalists in Myanmar.[21] Other countries where there are records of its use for extracting data from journalists, activists, and/or political opponents include Botswana, Ghana, Nigeria, Hong Kong, Bangladesh, Indonesia, India, Russia, Belarus, Venezuela, Bahrain, and Saudi Arabia.[22]

In the United States, the organisation UpTurn identified that the UFED solution, developed by Cellebrite,[23] was widely distributed, being present in all states of the country. However, its use had extended beyond serious offenses and was being directed at crimes such as vandalism, theft, prostitution, hit-and-run accidents, and all types of crimes related to illegal drugs. Due to this latter use, the study suggests a high possibility that these extractions disproportionately affected Black and Latinx people.

Such an inference can also be made in the Brazilian context. The previously mentioned Project Excel distributed Cellebrite devices to state public security secretariats. In a promotional video released by the Ministry of Justice and Public Security, the most investigated crime was drug trafficking, representing 66% of the offenses investigated. According to data from the Institute of Applied Economic Research (IPEA), Black individuals make up the majority of those arrested for drug trafficking in police rounds.[24] Therefore, it is highly likely that the data sent to the Project Excel databases has a racial bias, posing risks for public security policies that may be developed based on the processing of such information.

These abuses highlight the risks associated with the production and use of these tools. Their existence presupposes the creation and maintenance of vulnerabilities that put the data and information of various sectors of society at risk. This situation complicates the

---

[21] McLaughin, Tommy. Security-tech companies once flocked to Myanmar. One firms tools were used against two journalists. **The Washington Post**, 4 May, 2019. Available at 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 . Accessed on 04, December 2024.

[22] Krapiva, Natália; Hinako. What spy firm Cellebrite can't hide from investors. **AccessNow**, 26 May, 2021. Available at https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/ . Accessed on 04, December 2024.

[23] Koepke, Logan et al. **Mass Extraction**. UpTurn, 2020. Available at https://www.upturn.org/work/mass-extraction/ . Accessed on 04, December 2024.

[24] G1. Negros são maioria entre presos por tráfico de drogas em rondas policiais, diz IPEA. **G1**, 13 March, 2024. Available at https://g1.globo.com/politica/noticia/2024/03/13/negros-sao-maioria-entre-presos-por-trafico-de-drogas-em-rondas-policiais-diz-ipea.ghtml . Accessed on 05, December 2024.

maintenance of a secure and stable digital ecosystem for all, which is why it is essential to consider this context when developing any national cybersecurity policy.

Moreover, these intrusion tools pose a serious threat to human rights. As previously outlined, such tools are being employed to persecute activists, journalists, political dissidents, and social minorities. Therefore, beyond the right to privacy, rights such as freedom of expression, press, association, and even the right to life may be jeopardised due to tools like these. This threat arises not only from their use against specific targets but also from the potential for these tools to inhibit citizens from freely expressing themselves due to fear of surveillance and state repression (the chilling effect).

It is also important to note that once these tools are acquired, the intrusive arsenal will be available for use by both more democratic and more authoritarian leaders. Similarly, once within the state's framework, without proper regulation, safeguards, and transparency, there is a significant risk that these solutions will experience function creep.

Lastly, the widespread use of intrusion solutions within the Brazilian police forces raises concerns, particularly in cities with a high incidence of militias. Therefore, it is necessary to consider the possibility that intrusion tools may be used to extract data from citizens within militia-controlled areas as a means of territorial control and surveillance, further putting already socially vulnerable people at greater risk.

3. Legal and Regulatory Context

3.1. Current Brazilian Context

3.1.1. Federal Constitution

In Brazil, in addition to the right to privacy guaranteed by Article 5, Section X of the Constitution, which plays a central role in analysing rights that may be restricted through the use of tools for accessing and extracting data, the access to private communications is also protected by Section XII of the same article. Any action to access private information, including communications, must be carried out through procedural means that ensure legality, proportionality, and the demonstration of necessity. Furthermore, the need for judicial authorisation, properly substantiated, is essential.

Constitutional Amendment No. 115/2022 inserted into Article 5 (Section LXXIX) of the Brazilian Constitution, the fundamental and autonomous right to personal data protection. This means that infra constitutional norms and administrative instruments regulating the use of tools for accessing and extracting data must always consider the protection of the fundamental rights enshrined in the Constitution. Adherence to principles such as purpose, necessity, data quality, transparency, security, prevention,

and accountability of those responsible for data processing in access and extraction operations must be consolidated based on the constitutional right to personal data protection.

It is important to note that the protection of these rights extends beyond the individual sphere, especially when it comes to large-scale data collection, affecting services such as emails, social networks, instant messaging apps, and web browsers, encompassing entire communities whose data is being seized. Therefore, proportionality and necessity tests in the use of these tools must take into account the impact on the rights of other individuals, who are often not involved in a criminal investigation but will have their rights suspended due to investigative and surveillance routines of this nature.

3.1.2. The Civil Internet Framework (MCI)

The MCI establishes that a court order is required for the storage and access to connection records, application data, and the contents of communications (Article 7, II and III; Article 10, §§1 and 2; Article 15, §1). In other words, when applying the MCI, there is a legal procedure that must be followed by the entity responsible for the investigation when access to data and communications is intermediated by a service provider, whether for connection or application. However, when access is made directly to the device, without the participation of an intermediary, the MCI does not establish clear and specific guidelines, which can create room for arbitrariness, legal uncertainty, and abuse in monitoring. In any action of collection, storage, retention, and processing of records, personal data, or communications by connection providers and internet applications, when at least one of these acts occurs in Brazil, the MCI imposes the obligation to follow Brazilian legislation, guaranteeing the rights to privacy, personal data protection, and the secrecy of private communications and records.

3.1.3. General Data Protection Law (LGPD) and Criminal LGPD

Although the General Data Protection Law (LGPD) establishes rules regarding the use of personal data in both the public and private sectors, Article 4 of the LGPD excludes from its scope data processing for "public security, national defense, state security, and the investigation and repression of criminal offenses" (Section III, sub-sections "a" to "d"). Similar to the European Union’s General Data Protection Regulation (GDPR), Brazilian legislation provides exceptions in the context of public security. However, unlike the European regulation, which created a specific directive to address the penal sphere (Directive 2016/680), Brazil still does not have its own legislation that specifically addresses this issue.

3.1.4. Bill No. 402/2024

Bill No. 402/2024, authored by Senator Alessandro Vieira (MDB/SE), aims to regulate the use of remote monitoring tools for personal communication terminals by public agencies and agents, both civilian and military.

One of the key aspects of the bill is its emphasis on adherence to established principles such as legality, proportionality, necessity, security, transparency, and oversight, in line with those set forth in the Brazilian General Data Protection Law (LGPD). Additionally, the bill ensures that the use of these tools will be conditioned upon prior judicial authorisation. This requirement reinforces the need for protection against abuses.

It is important to note the scope of the bill, which goes beyond regulating the extraction of data from individual devices, also addressing mass data collection—an issue of increasing relevance given the evolution of large-scale surveillance technologies.

Another crucial point of the bill is the criminalisation of monitoring without judicial authorisation, as well as the obligation to report incidents related to failures or abuses in the use of these tools. These provisions represent a significant advancement in the creation of a robust legal framework aimed at ensuring accountability for public agents involved and preventing abuses of power. However, the bill does not address potential legal remedies available to victims of arbitrary surveillance.

While the bill presents important advances, it also requires further discussion regarding surveillance practices and oversight with multistakeholder participation. The inclusion of more details on the preparation of detailed reports to increase the transparency of the process is a point to be raised. The inclusion of measures to ensure due process of law is also essential in order to prevent violations of the chain of custody, given that these tools have the potential to alter the contents of infected devices.

Finally, the bill fails to include a provision that would prevent the state from establishing commercial relationships with companies involved in human rights violations, both domestic and foreign. Creating a list of companies that meet these criteria and prohibiting state dealings with these entities would strengthen Brazil's commitment to fundamental rights and national sovereignty.

It is important to emphasize that, although the bill represents an excellent opportunity to engage in a thorough discussion on this topic, it does not address the need for a penal LGPD, which would provide a comprehensive legal framework for the protection of

personal data in the context of public security, national security, and state defense. Therefore, the two proposals would be complementary, not mutually exclusive.

In summary, Bill No. 402/2024 represents a significant advancement in the regulation of surveillance practices in Brazil, offering a legal model aimed at balancing privacy rights with the need for public security. If implemented effectively, the bill could position Brazil as a global leader in the protection of digital rights, inspiring similar legislation in other countries, much like the impact of the Civil Internet Framework.

3.1.5. Argument of Non-Compliance with Fundamental Precept (ADPF) 1143

Argument of Non-Compliance with Fundamental Precept (ADPF) 1143 addresses a challenge raised by the Attorney General's Office (PGR) regarding the lack of regulation on the use of surveillance software by public agencies. Initially, the issue was brought before the Federal Supreme Court (STF) through Direct Action of Unconstitutionality for Omission (ADO) 84, in which the PGR criticised the absence of normative action by the National Congress to regulate this matter. The PGR argued that these technologies have been used by intelligence and state repression agencies to conduct remote and invasive surveillance of mobile devices, under the guise of combating terrorism and organised crime. The action was later converted into ADPF 1143 at the request of the Attorney General's Office itself.

In early 2024, Minister Cristiano Zanin, the rapporteur for the case, requested information from the National Congress and sent the case to the Federal Attorney General's Office (AGU) and the PGR. In April of the same year, the Minister ordered the holding of a public hearing, aimed at gathering technical and empirical information on the subject, which was scheduled for June 10 and 11. IP.rec participated in this hearing and provided several relevant contributions to the discussion.

In May 2024, Minister Cristiano Zanin of the Federal Supreme Court (STF) ordered the Courts of Accounts of the Union, states, and municipalities to provide information on any administrative proceedings related to tenders, acquisitions, or contracts for spyware for personal communication devices, such as mobile phones and tablets. Regarding the tracking programs, the Minister clarified that the tools in question include, but are not limited to, Pegasus, IMSI catchers (such as Pixcell and G12), and applications that monitor the location of specific targets, like First Mile and Landmark. By November 2024, more than 20 Courts of Accounts had submitted documents to the court.[25]

[25] https://portal.stf.jus.br/processos/detalhe.asp?incidente=6900814

3.2. Legislation and Relevant International Precedents

3.2.1. Legislation and Initiatives

a) U.S. Initiatives

In 2021, the U.S. Department of Commerce announced the inclusion of spyware companies in its "Entity List," a list that compiles individuals, companies, and foreign organisations considered a threat to U.S. national security. This inclusion subjects them to export restrictions and licensing requirements for specific technologies and products. In that year, Israeli spyware companies NSO Group and Candiru were added to the list.[26] In 2023, the list was expanded to include Intellexa, based in Greece and Ireland, and Cytrox AD, headquartered in Hungary and North Macedonia.[27]

In 2024, the Canadian company Sandvine was added after its products were used for mass web surveillance, censorship, and attacks on human rights activists and dissidents, including the misuse of commercial spyware. However, in October 2024, the company was removed from the list after implementing a series of measures to address the improper use of its technology. Among the actions taken were corporate restructuring, changes in leadership, and modifications to the business model, focusing on serving democracies committed to human rights protection. The company also pledged to exit non-democratic countries, with 32 already abandoned and 24 others in the process of withdrawal. The U.S. government further mentioned "strengthening relations with civil society," "allocating profits for rights protection," "including human rights experts in the new leadership team," "evaluating business decisions through the newly created Corporate Ethics Committee," and "rigorous monitoring of the misuse of technology in countries where the company intends to remain."[28]

---

[26] U.S. Department of Commerce. Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities. 2021. Available at https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list Accessed on 10 Dec, 2024

[27] U.S. Department of State. The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities. 2023. Available at https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities-2/ Accessed on 10 Dec, 2024

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

In March 2023, during the second Summit for Democracy organised by the United States, 11 countries signed a joint declaration acknowledging the threat posed by the misuse of commercial spyware. They highlighted the urgent need to establish strict controls, both national and international, to curb the proliferation of these tools. The declaration was later updated to include new countries that joined the multilateral commitment to combat the abusive use of these technologies. In March 2024, during the third Summit for Democracy, countries such as Finland, Germany, Japan, Poland, Ireland, and South Korea reinforced their support for concrete measures to address the risks associated with the use of commercial spyware.[29]

The declaration emphasises that commercial spyware has been misused by both authoritarian regimes and democracies, often to persecute political opponents, intimidate dissidents, suppress freedom of expression, and violate human rights. In response, the signatory countries committed to adopting strict measures to ensure that the use of spyware by their governments aligns with human rights, the rule of law, and civil liberties. Additionally, the countries pledged to implement robust export control practices to prevent the transfer of technologies to users who may employ them for "malicious activities."

However, practical experience has shown that these controls are often easily circumvented or not rigorously enforced, as pointed out in investigations conducted by members of the European Parliament.[30] Although the commitment to increased international cooperation and information sharing regarding the misuse of spyware is positive, there is still a lack of clear and effective mechanisms to ensure that these measures lead to a tangible impact on curbing the proliferation of this technology.

In summary, while the March 2023 declaration represents progress in recognising the problem, the concrete actions taken so far do not reflect the magnitude of the threat. The Trump administration is unlikely to continue the Biden administration's campaign to limit the proliferation of commercial spyware technologies, which are widely used by authoritarian regimes to persecute journalists, civil rights activists, and political opponents. Trump and his allies maintain close political and financial ties with two of the largest consumers of these tools, Saudi Arabia and the United Arab Emirates,

---

[29] The White House. Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware. **The White House.** 2024. Available at https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/18/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/ Accessed on 10 Dec, 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**. Available at https://www.europarl.europa.eu/doceo/document/PEGA-RD-740554_EN.pdf Accessed on 10 Dec, 2024

demonstrating a negligent stance regarding the human rights violations of these regimes.

According to Steven Feldstein from the Carnegie Endowment for International Peace, it is highly likely that there will be setbacks in spyware control policies, with the Trump administration prioritising the counterterrorism arguments presented by spyware companies over the criticisms from digital rights advocates.[31] In this context, companies like NSO Group, which have close ties with the Israeli government aligned with Trump, are expected to find a more favorable environment for their operations.

Media outlets reported that by October 2024, NSO had spent over $1.8 million on lobbying, according to documents from the Foreign Agents Registration Act.[32] The company has focused its efforts on establishing connections with Republican lawmakers and has continued its push to use the context of the Israel war to increase its chances of resuming its activities. It even promoted itself as a volunteer in the Gaza war, claiming to help locate missing Israelis and hostages. This attempt to convince the U.S. government to allow its return was seen as a "reputation laundering" strategy by NSO.

b) Pall Mall Process

In February 2024, the governments of the United Kingdom and France launched the Pall Mall Process (PMP) in London, an initiative focused on dialogue regarding the "proliferation and irresponsible use of commercial cyber intrusion capabilities."[33] The resulting declaration from the initial event emphasised guiding principles such as accountability, accuracy, oversight, and transparency, highlighting the importance of public-private partnerships and multistakeholder collaboration, as well as expressing concerns about national security, human rights, and fundamental freedoms. Moreover,

---

[31] Eric Geller. More Spyware, Fewer Rules: What Trump's Return Means for US Cybersecurity. **Wired**. 14 November, 2024. Available at https://www.wired.com/story/trump-administration-cybersecurity-policy-reversals/ Accessed on 10 Dec, 2024

[32] Georgia Gee. Pegasus spyware maker said to flout federal court as it lobbies to get off U.S. blacklist. **The Intercept**. 21 October, 2024. Available at https://theintercept.com/2024/10/21/pegasus-spyware-nso-israel-lobbying-republicans/ Accessed on 10 Dec, 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.** Available at 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 Accessed on 10 Dec, 2024

the discussion process, conducted behind closed doors and without the presence of media outlets, raises questions about transparency and the inclusion of diverse actors and perspectives. This lack of visibility could limit the event's impact and reduce public trust in the integrity of the process.

Another issue to note is the absence of countries that are major producers of cyber intrusion tools, such as Israel, as well as companies supplying these resources. The absence of these key actors may hinder the effective implementation of the principles established, as international governance over the use of such technologies largely depends on the commitment of the parties involved in the production and commercialisation of these tools.

Finally, the limited participation of civil society organisations represents a significant gap in a process that aims to be multistakeholder. These organisations play a crucial role in shedding light on an opaque cybersecurity market, and their inclusion in such discussions is essential to ensure transparency and fairness in decisions that impact digital rights and global security.

In summary, while the PMP represents an important step forward in addressing critical cybersecurity issues, its future effectiveness will depend on expanding international participation, increasing transparency in the process, and the active inclusion of all relevant sectors, including global actors and civil society organisations.

3.2.2. Precedents

Although legal cases can be based on leaked information or digital forensic analyses that identify characteristic signs of the use of intrusion tools, the lack of a comprehensive, accessible, reliable, and complete record of operations carried out with these technologies by governments makes it difficult for victims to prove their claims, as well as for judicial authorities to conduct proper investigations into all circumstances. The number of granted requests filed by those affected by the illegal use of digital tools (both individual victims and technology companies whose systems were unlawfully breached) remains limited in Brazilian jurisdiction. However, in recent years, there has been an increase in cases directly related to the use of these tools to monitor and persecute journalists and human rights defenders, particularly in various regional human rights protection courts.

In March 2024, in a historic ruling in the case *Members of the José Alvear Restrepo Lawyers Collective (CAJAR) v. Colombia*,[34] the Inter-American Court of Human Rights identified a violation of the right to privacy and emphasised the tensions that technological development and the widespread circulation of data bring to the realm of human rights protection. The Court thus highlighted the importance of judicial authorisation, independent oversight of intelligence activities, and the need for effective solutions. The decision also determined that intelligence operations—such as those involving spyware and malware, among other technologies—are only legal and valid when accompanied by robust controls and safeguards. Echoing its previous judgment in *Escher et al. v. Brazil*,[35] the Court emphasised that protecting privacy and freedom of expression is fundamental, and any surveillance measures must be authorised by a judicial authority that defines their scope, duration, and limits.

In Europe, in the case *Pietrzak and Bychawska-Siniarska and others v. Poland*, in May 2024, the European Court of Human Rights (ECHR) unanimously concluded that Poland's 2016 surveillance law violated Article 8 of the European Convention on Human Rights, which safeguards the right to privacy. The Court identified three key issues with the law, particularly related to the use of commercial spyware such as Pegasus: (i) the lack of adequate safeguards, such as the absence of a requirement for judicial authorisation and remedies; (ii) excessively broad retention of communication data; and (iii) inadequate oversight. Also in Europe, in the cases *Liberty and others v. the United Kingdom*, *Roman Zakharov v. Russia*, and *Pietrzak and Bychawska-Siniarska and others v. Poland*,[36] the lack of effective oversight and available remedies under national law for those subjected to covert digital surveillance tools, such as spyware by state agencies, was considered a violation of Article 13 of the European Convention on Human Rights, which ensures the right to an effective remedy in cases of human rights violations.

---

[34] **Inter-American Court of Human Rights**, *Members of the Corporación Colectivo de Abogados "José Alvear Restrepo" v Colombia*, Judgment of 18 October 2023, Inter-American Court of Human Rights, available at: https://privacyinternational.org/sites/default/files/2024-03/seriec_506_esp.pdf, accessed 10 December 2024.

[35] **Inter-American Court of Human Rights**, *Escher and Others v Brazil*, Judgment of 6 July 2009, Judgment of 20 November 2009, Inter-American Court of Human Rights, available at: https://www.corteidh.or.cr/docs/casos/articulos/seriec_208_por.pdf, accessed 10 December 2024.

[36] **European Court of Human Rights**, *Pietrzak v Poland and Bychawska-Siniarska and Others v Poland*, available at: https://hudoc.echr.coe.int/eng#{"itemid":["002-14333"]} , accessed 10 December 2024.

4. Best Practices and Guidelines for the Acquisition and Use of Technologies by the Federal Government

4.1. National Sovereignty and Provenance of Acquired Technologies

As noted by the European Parliament's Inquiry Committee, which investigates the use of Pegasus and equivalent surveillance spyware, countries in the Global North are seen as attractive locations for the headquarters of technology and surveillance service companies.[37] According to recent studies, major suppliers of digital intrusion tools, such as Cellebrite, FinFisher, Blue Coat, Hacking Team, Nexa Technologies, CyberPoint, L3 Technologies, Verint, Sandvine, and NSO Group, are based in countries considered democratic, such as the United States, Italy, France, Germany, Canada, and Israel.[38] Nevertheless, many of these companies have supplied technologies both to autocratic regimes and for the illegitimate use by democratic governments around the world.

Since 2022, however, there has been a shift in the discourse of various governments regarding the need to develop a regulatory framework aimed at curbing the proliferation and threat posed by the "misuse" of digital intrusion tools. In this context, we believe that Brazil needs to implement stricter controls over the importation of these tools to prevent them from being developed by or acquired from actors who violate or contribute to the violation of human rights, or who jeopardise national sovereignty.

Considering the evident risks to human rights and the challenges of oversight, former UN Special Rapporteur on Freedom of Expression, David Kaye, proposed a moratorium on the trade of surveillance technologies, with the goal of "allowing States to develop an export control regime and strengthen the legal frameworks that protect privacy."[39] This call was supported by several UN Special Procedures mandate holders. In 2022, Costa

---

[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**. Available at https://www.europarl.europa.eu/doceo/document/PEGA-RD-740554_EN.pdf Accessed on 10 Dec, 2024.

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

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

Rica became the first country to request the implementation of this moratorium.[40] Therefore, it is essential that the Brazilian government considers the possibility of a moratorium on the purchase of certain private surveillance equipment with higher intrusive capabilities, until clear and responsible regulations are established. This measure is justified by the severity of the damage caused by these technologies.

Finally, it is important to note the advancements in other jurisdictions. Companies like Meta and Apple have already sued suppliers of intrusion tools, such as NSO Group, due to the use of software like Pegasus against their users.[41] The Israeli group argued that, since its products are used by foreign governments and law enforcement agencies, it should be protected by sovereign immunity on U.S. soil. However, the Ninth Circuit Court of Appeals rejected this claim, creating an important precedent for the accountability of spyware companies.[42] The decision allowed for a legal case to be filed against the company, marking a significant development in the discussion on responsibility in the use of such technologies.

4.2. Guarantees of Transparency and Monitoring and Audit Mechanisms

Evidence, such as that presented in our study "Merchants of Insecurity: The Context and Risks of Government Hacking in Brazil," makes it imperative that the Brazilian government be transparent about its efforts to ensure that national security and investigative services operate in compliance with fundamental rights and civil liberties. During data collection by IP.rec researchers for our study, using Transparency Portals and requests grounded in the Freedom of Information Act, it was found that the level of transparency regarding the acquisition of these tools by public bodies is still considered low.

Additionally, bodies responsible for oversight and supervision, such as the National Data Protection Authority (ANPD) and audit courts, should not face difficulties in

---

[40] Access Now. Stop Pegasus: Costa Rica is the first country to call for a moratorium on spyware technology. 2022 Available at https://www.accessnow.org/press-release/costa-rica-first-country-moratorium-spyware Accessed on 10 Dec, 2024.

[41] Stephanie Kirchgaessner. Court orders maker of Pegasus spyware to hand over code to WhatsApp. **The Guardian**. 29 February 2024. Available at https://www.theguardian.com/technology/2024/feb/29/pegasus-surveillance-code-whatsapp-meta-lawsuit-nso-group Accessed on 10 Dec, 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. **International Justice Clinic**. Available at 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/ Accessed on 10 Dec, 2024

obtaining this information. Independent oversight of intelligence services and the acquisition of intrusion tools in Brazil is notoriously weak and often non-existent. It is essential that both ex-ante and ex-post scrutiny mechanisms be strengthened. The creation of an independent oversight mechanism for the use of these technologies is urgent and necessary. Measures like these would establish more effective ways to protect the rights and civil liberties of the population.

It is crucial that the Brazilian government ensures that allegations of illegal monitoring and abuse of intrusion tools are adequately investigated and that those responsible are held accountable when necessary. Clear rules must also be established to limit the use of "national security" as a justification for surveillance, ensuring appropriate judicial oversight and respect for fundamental freedoms and guarantees.

It is important to emphasise that digital intrusion tools are not isolated in this scenario but are part of an entire network of institutions and actors. The use of these tools often depends on the (non)existence of regulatory measures, legal safeguards, and oversight mechanisms. As noted by the European Parliament, regulatory systems have often, intentionally or unintentionally, been distorted, either partially or entirely, or designed in a way that facilitates the use of highly intrusive monitoring mechanisms.[43] Thus, the illegitimate or abusive use of these tools stops being an isolated incident and becomes a strategy. Therefore, it is recommended that the Brazilian government base the use of these tools on a precise and specific legal framework, with robust scrutiny mechanisms.

Legal remedies must also exist and be effective when faced with obstruction by government bodies. As noted by Ní Aoláin, States often establish separate judicial systems, such as "secret courts," to deal with national security cases.[44] Surveillance activities carried out by state agencies make traditional accountability mechanisms more difficult. Additionally, the transnational transfer of technology presents specific jurisdictional and practical challenges. The Brazilian government should not allow the involvement of private entities in the development and operation of these intrusion tools to further hinder access to effective remedies for addressing human rights violations.

---

[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**. Available at https://www.europarl.europa.eu/doceo/document/PEGA-RD-740554_EN.pdf Acessed on 10 Dec, 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.** April, 2023. Available at 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

4.3. Training and Specialisation of Responsible Authorities

The right to a fair trial is a crucial element of the Rule of Law. States ensure this right not only by guaranteeing the independence of judges and courts but also by preserving the integrity of digital evidence and ensuring that both the prosecution and defense have equal access to relevant information, including data on the chain of custody.[45]

The training and specialisation of authorities responsible for administering justice and protecting fundamental rights are essential to ensuring the integrity of the judicial process, especially in a context where digital evidence plays a central role. The case *Rook v. Germany*, analysed by the European Court of Human Rights, exemplifies the challenges arising from the use of digital technologies in judicial processes, highlighting the violation of the right to a fair trial due to failures in preserving and accessing digital evidence, including the chain of custody. The integrity of this evidence is fundamental to ensuring that the defense's rights are respected and that the evidence can be meaningfully contested, as emphasised by the Court.

The issue of data protection and the preservation of digital evidence was also highlighted by the former UN Special Rapporteur on freedom of expression, David Kaye, who warned about the risks of tampering with digital records through the use of tools such as spyware.[46]Certain digital intrusion tools, by allowing the discreet alteration of data without leaving traces, represent a grave threat to the impartiality of the judicial process and the right to a fair trial, as they can be used by both state actors and other agents to intentionally or accidentally modify information. The use of such tools, therefore, demands strict regulation and specific training for the agents involved, in order to mitigate the risks of evidence manipulation.

The evolution of surveillance technologies, such as Pegasus, requires adaptation within the global regulatory framework. The push for a more robust legal system aims to recognise that certain intrusion tools, due to their inherent characteristics, should not be used in judicial proceedings, as their ability to alter data without leaving traces

---

[45] European Court of Human Rights, *Rook v Germany* (25 July 2019) https://hudoc.echr.coe.int/eng#{"itemid":["001-194614"]} Accessed on 10 Dec, 2024

[46] David Kaye e Sarah McKune. The Scourge of Commercial Spyware—and How to Stop It. **Lawfare**. 2023. Available at https://www.lawfaremedia.org/article/the-scourge-of-commercial-spyware-and-how-to-stop-it Accessed on 10 Dec, 2024

compromises the principle of the integrity of evidence.[47] The European Data Protection Supervisor emphasised that intensified digital surveillance and associated tools, by changing the dynamics of investigation and judgment, require highly qualified authorities who can ensure the legitimate use of these technologies within the limits of the Rule of Law.[48]

Therefore, the technical training and specialisation of Brazilian authorities responsible for the collection, preservation, and analysis of digital evidence are crucial to ensuring that the judicial process is not compromised by the improper use of these tools. International collaboration between Brazil and different jurisdictions, aimed at exchanging knowledge and best practices, is equally necessary so that authorities can effectively respond to the challenges posed by digital surveillance and the integrity of evidence, thereby preserving human rights and the Rule of Law.

4.4. Participation of Civil Society and Experts on the Topic

In recent years, the active participation of civil society has been crucial in shedding light on the ethical implications and abuses associated with the use of digital intrusion tools. Non-governmental organisations, journalists, and activists have played a key role in exposing the misuse of these technologies, often in authoritarian regimes or for indiscriminate surveillance in democracies. However, despite their critical contribution to raising awareness of the problem, civil society remains marginalised in discussions around the regulation and accountability of these actions, often to the detriment of a more technical and transparent approach.

The lack of effective participation from civil society and specialists in the field undermines the process of formulating public policies aimed at protecting fundamental rights such as privacy and freedom of expression. Experts in technology, human rights, and digital security have stressed the need to create a more inclusive and participatory regulatory environment, where different voices can be heard. Thus, the participation of civil society and experts is essential to ensure a balance between security and freedom, as well as to ensure that the adopted norms align with democratic principles and human rights.

---

[47] Fionnuala Ní Aoláin. United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. **United Nations.** April 2023. Available at 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 Accessed on 10 Dec, 2024

[48] European Data Protection Supervisor. EDPS Preliminary Remarks on Modern Spyware. 2022. Available at https://www.edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en Accessed on 10, Dec, 2024.

The contribution of experts in areas such as digital rights is crucial to ensure that the regulation of the use of digital intrusion tools is based on robust technical knowledge and a human rights approach. In Brazil, an interdisciplinary and transparent debate is essential so that the process of formulating public policies is not solely dominated by economic or security interests, but also considers the social and individual impacts of using these technologies. The creation of an inclusive and participatory regulatory environment ensures that the norms adopted are aligned with democratic principles and human rights, avoiding abuses and excesses in the use of digital intrusion tools, which can be easily misused for indiscriminate surveillance, as evidenced by the work of IP.rec, journalists, and other civil society representatives. Therefore, collaboration between civil society and public authorities is essential for building a more just and effective control system over the use of these technologies in Brazil.

5. Challenges and Final Considerations

There is a constant challenge in balancing the protection of citizens with guaranteeing human rights. At times, the State uses the narrative of protection to introduce intrusion and surveillance equipment, when in reality, they pose greater risks and insecurity.

The technological development of digital solutions creates technical flaws. Even if unintentional, the emergence of new vulnerabilities creates larger areas of attack for malicious actors. Often, these flaws are unknown to the development team, who only become aware of them later. As a result, intrusion companies and bug bounties commercially exploit these flaws, while States use them for intelligence purposes.

In this context, advances in cybersecurity are necessary for corrections, as this field advances in research of new protection techniques, offering ever-higher levels of security. However, on the other hand, intrusion solutions also advance, developing and identifying new ways to bypass defense mechanisms, creating a circular scenario of insecurity that seems to grow increasingly.

Therefore, in light of the rapid technological development, constant updates to cybersecurity policies and regulations for digital intrusion tools are needed. All improvements should take this context into account to create a safer environment for users.

In the face of these challenges and technological advancements, it is essential that Brazil adopts a proactive approach to protect its citizens, promoting transparency in surveillance operations and ensuring that any use of digital intrusion tools is adequately monitored.

The strengthening of legal frameworks, supervision mechanisms, and the inclusion of various sectors of society, including experts and civil organisations, is crucial to ensure that the use of these technologies is transparent, responsible, and aligned with democratic principles. In Brazil, it is essential that the government adopts strict measures to control the importation and use of these tools, ensuring that they are not employed in the violation of fundamental rights or in ways that threaten national sovereignty.

Furthermore, the training of authorities responsible for investigating and analysing digital evidence, transparency in the acquisition of surveillance technologies, and the implementation of effective control over their use are fundamental to ensuring that the rights of the population are protected, and that the use of digital technologies is in compliance with the Democratic Rule of Law.

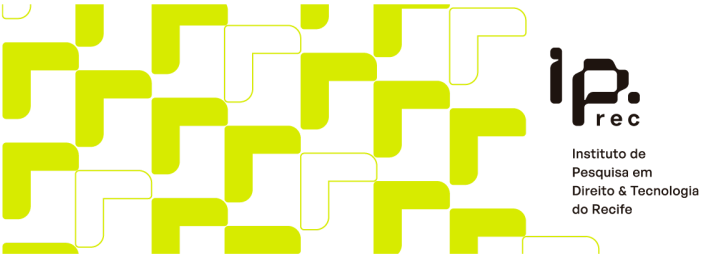
6. Recommendations

Promotion of transparency in public procurement processes:
It is recommended to increase transparency in public procurement processes regarding the acquisition of products and the hiring of services related to digital intrusion tools from private companies, while observing potential issues related to human rights and to public and national security.

Guaranteeing transparency in the use of digital intrusion tools:
It is recommended that, in cases of the use of digital intrusion tools, full transparency should be promoted to ensure compliance with legal and ethical standards, while preserving public trust and protecting fundamental rights and civil liberties.

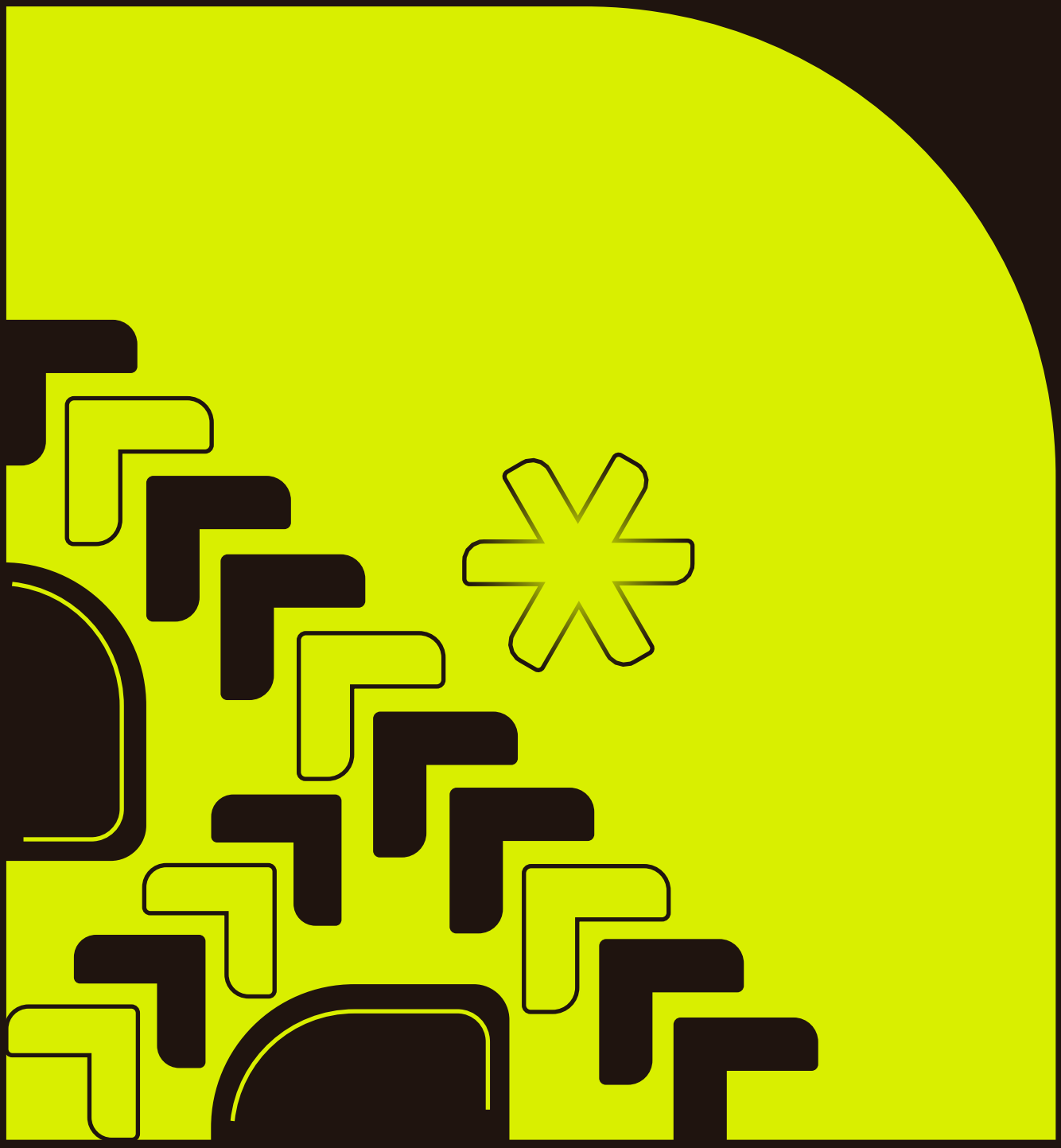
Observance of human rights by contracted companies:
It is recommended not to engage with companies involved in the surveillance and collection of information about activists, academics, journalists, dissidents, political figures, or members of non-governmental organisations or marginalised communities, with the aim of limiting freedoms of expression or enabling human rights abuses or the suppression of civil liberties.

Ban on intrusive tools without reliability criteria:
It is recommended to ban the purchase and use of digital intrusion tools (especially remote ones) that lack characteristics of auditability, transparency, and specificity, such as Pegasus.



Implementation of a moratorium on highly intrusive tools:
It is recommended to implement a moratorium on the use and acquisition of highly intrusive digital tools until appropriate regulations on the matter are developed.

Approval of the General Data Protection Law for Criminal Purposes:
It is essential to approve a General Data Protection Law for public security, national defense, and intelligence purposes, in order to guarantee the protection of privacy and individual rights.



Instituto de
Pesquisa em
Direito & Tecnologia
do Recife