DataPrivacyBR Research

INTERNETLAB
pesquisa em direito e tecnologia

# AMICUS BRIEFING

## PRESENTED TO THE BRAZILIAN SUPREME COURT

## BY DATA PRIVACY BRASIL AND INTERNETLAB

## CASE ADPF 1143

## CONSTITUTIONAL LIMITS OF SPYWARES

2024

DataPrivacyBR Research

INTERNETLAB
pesquisa em direito e tecnologia

**HONORABLE JUSTICE CRISTIANO ZANIN OF THE BRAZILIAN SUPREME COURT**

Action Against the Violation of a Constitutional Fundamental Right No. 1143

INTERNETLAB ASSOCIATION FOR RESEARCH IN LAW AND TECHNOLOGY ("InternetLab"), and the DATA PRIVACY BRAZIL RESEARCH ASSOCIATION ("Data Privacy Brazil"), duly identified in the record, respectfully come before Your Honor, by their duly constituted attorneys, pursuant to Article 138 of the Code of Civil Procedure, *to present their contribution as amici curiae,* for the arguments set out below.

# TABLE OF CONTENTS

# I. SUBJECT MATTER OF THE ACTION

1. This is an Action Against the Violation of a Constitutional Fundamental Right presented by the Office of the Chief Prosecutor of Brazil (hereinafter referred to as the PGR) seeking to prevent and remedy violations of fundamental rights by the Government. These violations are represented by the partial omission in regulating the use, as well as the indiscriminate acquisition and use, by public bodies and agents, **of remote virtual intrusion programs and secret and invasive monitoring tools** for personal digital communication devices.

2. In effect, the present action – initially proposed as a Direct Action for the Declaration of Unconstitutionality by Omission (ADO) No. 84 and converted into the Action Against the Violation of a Constitutional Fundamental Right (ADPF) No. 1143 – aims to provide complete effectiveness and to confer adequate protection to the mandates set out in Article 5, items X, XII and LXXIX of the Constitution of the Federative Republic of Brazil[1], in view of recent technological advances, which have culminated in the global proliferation of virtual intrusion tools. These tools have been used by intelligence services, state repression agencies and national defense agencies for remote, secret, and invasive surveillance of mobile digital communication devices, under the pretext of countering terrorism and organized crime.

3. In short, the PGR's initial request seeks to correct the insufficiency of the country's legal system in providing adequate protection for the guarantee of the inviolability of private life, intimacy and secrecy of personal communications and data on personal digital communication devices, in view of the new tools and systems for infiltration and remote virtual intrusion used by public bodies and agents in the course of investigations and ongoing intelligence activities.

**1** "Article 5. All persons are equal before the law, without any distinction whatsoever, Brazilians and foreigners residing in the country being ensured of inviolability of the right to life, to liberty, to equality, to security and to property, on the following terms: [...] X – the privacy, private life, honor and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured; [...] XII – the secrecy of correspondence and of telegraphic, data and telephone communications is inviolable, except, in the latter case, by court order, in the cases and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts; [...] LXXIX – under the terms of the law, the right to protection of personal data is guaranteed, including in digital media".

4. To this end, the action filed to this Court sought to (i) declare the unconstitutionality of the partial omission of the Brazilian Congress in making fully effective the mandates for the protection of intimacy and private life, and the inviolability of the secrecy of personal communications and data, set out in Article 5, items X and XII, of the Brazilian Federal Constitution, by regulating the use, by public bodies and agents, of remote virtual intrusion programs and secret and invasive monitoring tools for personal digital communication devices - smartphones, tablets and similar electronic devices; (ii) setting a reasonable deadline for the Brazilian Congress to remedy the legislative delay; and (iii) establishing provisional guidelines to safeguard the fundamental rights to intimacy and privacy, and the inviolability of the secrecy of personal communications and data, until the unconstitutional regulatory gap is remedied.

5. In this context, InternetLab and Data Privacy Brazil have requested to be included as *amici curiae* in this Action Against the Violation of a Constitutional Fundamental Right (ADPF) No. 1143, then a Direct Action for the Declaration of Unconstitutionality by Omission (ADO) No. 84, so that they can contribute to the constitutional debate at hand, bringing legal, theoretical and technical elements capable of providing information for a decision to be made by this Supreme Court.

6. On April 16, 2024, Reporting Honorable Justice Cristiano Zanin admitted InternetLab and Data Privacy Brazil as *amici curiae*, considering the relevance between the institutional purposes of the entities and the subject matter of the lawsuit. In addition, the Honorable Justice called a public hearing to be held on June 10 and 11, 2024, in order to hear from experts on the subject. Both entities took part in the hearing and made their contributions to the debate before the Court. Furthermore, it was decided to convert the then ADO No. 84 into an Action for the Violation of a Constitutional Fundamental Right (ADPF), since the action is of a plural and heterogeneous nature, involving a set of acquisitions and the indiscriminate use of virtual intrusion tools.

7. As such, InternetLab and Data Privacy Brazil hereby present their contribution as *amici curiae*, gathering data and research conclusions to present to the Brazilian Supreme Court (STF):

*(i) the classification and organization of spyware, programs for intrusion on digital devices and communications;*

*(ii) the reasoning that the indiscriminate use of these technologies by the State is unconstitutional; and*

*(iii) subsidies for the assessment of the case in light of the constitutional interpretation of the protection of privacy and intimacy, the secrecy of data and communications, and the right to the protection of personal data contained in Article 5, items X, XII and LXXIX of the Brazilian Federal Constitution.*

## II. THE INTERNATIONAL VULNERABILITY EXPLOITATION INDUSTRY: CLASSIFICATION AND COMMON USES OF SPYWARES

8. In order to delve into the legal consequences of using and obtaining spyware, we must first examine what these tools are and how they fit into a global industry of exploiting vulnerabilities in information systems and protocols. The following paragraphs will provide such an overview.

9. **Spywares are, in general terms, tools (software) with intrusive capabilities for extracting information and invading electronic and communications devices or systems,** built from the exploitation of security flaws that may exist in these devices or in networks and information protocols through which communication flows. The user, owner or operator of the system is unlikely to be aware of the installation of spyware since these tools are intentionally built with the purpose of being invisible.

10. As noted by Fionnuala Ní Aoláin, professor of public law at the University of Minnesota Law School and UN Special Rapporteur on Counterterrorism, spyware today requires international cooperation for a legal framework that can avoid gaps in the existing framework in terms of supervision and *accountability*. The few legal initiatives are insufficient to adequately protect rights. According to Ní Aoláin, "*Spyware technology is currently being produced and deployed without a rigorous regulatory framework capable of responding to its unique characteristics*

*and substantial threat to human rights"*[2]. **Spyware is an intrusive technology for monitoring the content of individuals' digital communications and other information, including metadata** (location, duration, source, and contacts). Thus, "information extraction" refers to a wide range of data types.

**11.** A **vulnerability**, in turn, can be defined as "a set of conditions or behaviors that allows an explicit or implicit security policy to be violated"[3]. Vulnerabilities can arise at any stage, from software design to deployment, and can have various technical causes. These include software flaws, misguided design, or configuration decisions, as well as unforeseen interactions between systems and environmental conditions[4]. In software engineering, it is indisputable that **vulnerabilities will always exist, as well as the fact that these flaws expose systems and users of these products to significant risks**[5].

**12.** As these vulnerabilities are not communicated, either to device and software manufacturers or to the public, their discovery and exploitation is the gateway to targeted surveillance[6]. **In other words, the development, purchase, and sale of these technologies creates a veritable market for exploiting security vulnerabilities in communications**. According to author Ní Aoláin, the main private sector companies developing spyware are the NSO (Israel), Quadream (Israel), Candiru/Saito (Israel), Gamma International Ltd (UK), Vilicius Holding GmbH (Germany), Trovicor GmbH (Germany), Qosmos (France), Amesys (France), Area SpA (Italy), Hacking Team (Italy), Cytrox (Macedonia), Cyberpoins (USA), BlueCoat Systems (USA), Cisco Systems (USA), among others[7].

**2** NÍ AOLÁIN, Fionnuala. *Global regulation of the counter-terrorism spyware technology trade: scoping proposals for a human-rights compliant approach*. Office of the High Commissioner for Human Rights. Geneva: United Nations, 2023, p. 8. Available at: https://repository.graduateinstitute.ch/record/301602?v=pdf

**3** HOUSEHOLDER, Allen D. et al. *The cert guide to coordinated vulnerability disclosure. Software Engineering Institute: Cert Coordination Center (Carnegie Mellon University)*. Available at: https://certcc.github.io/CERT-Guide-to-CVD/, p.3

**4** *Ibidem*, p. 7.

**5** *Ibidem*, p. 2.

**6** SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION. *Surveillance and Human Rights*. United Nations Human Rights. May 28th, 2019. Available at: https://digitallibrary.un.org/record/3814512?v=pdf.

**7** NÍ AOLÁIN, Fionnuala. *Global regulation of the counter-terrorism spyware technology trade: scoping proposals for a human-rights compliant approach*. Office of the High Commissioner for Human Rights. Geneva: United Nations, 2023, p. 20. Available at: https://repository.graduateinstitute.ch/record/301602?v=pdf

13. There are two main ways in which governments can access these tools. The first is by developing monitoring software in their own intelligence agencies and departments, or by reinventing existing investigative tools. **The second, and most common, is by ordering and acquiring advanced spy software offered by companies that are part of the international surveillance industry**.

14. To this end, the report "Surveillance and Human Rights"[8], developed by the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, mobilized a series of analyses around the world on targeted state surveillance. The submissions showed that most of the targeted surveillance technologies used by governments come from the private sector. In general, **these companies sign secretive agreements with authorities interested in these tools**.

15. **The lack of transparency from governments and companies that exploit security vulnerabilities results in a striking consequence: it hinders public understanding of the problem**. From this perspective, most of the information we have on security vulnerabilities results from the investigative work of civil organizations and independent researchers[9].

16. The vulnerability industry's operations are considerably more obscure than, for example, ordinary government procurement processes. **The lack of transparency is crucial for this type of business to achieve its main objective**, which consists of the **silent surveillance of specific targets made possible by exploiting security flaws in technologies used by the majority of citizens**. Thus, by not being transparent about these products/services and the negotiation over them, states prevent these vulnerabilities from being discovered and corrected, creating a vicious cycle.

17. This vicious cycle produces technologies that are more susceptible to surveillance and less secure **in general**, as there is no guarantee that vulnerabilities will only be exploited for legitimate purposes. Thus, the absence or weakness of controls on the export and transfer of technologies that exploit the vulnerabilities explained

8 SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION. *Surveillance and Human Rights*. United Nations Human Rights. May 28th, 2019.

9 *Ibidem*, p. 2-3.

above is a catalyst for vigilantism, which is reinforced by governments with autocratic tendencies[10]. David Kaye[11] and Marietje Schaake discuss the dynamics of this market[12]:

> *They sell and service their products to government clients without regard for those governments' standards of repression and without adequate transparency and due diligence.* ***We are on the precipice of a global surveillance technology catastrophe, an avalanche of tools shared across borders, with governments unable to restrict their export or use[13].***

18. As a result, the global security vulnerability industry is supported by the opaque practices of states, and both imply a less secure and reliable information environment for all citizens. These services and products have significantly impacted the democratic environment, as well as the freedom of the press and freedom of expression.

19. **This impact needs to be illustrated**. As an example of a case that has gained international repercussions in this regard, we will discuss the **Pegasus software**, developed by the Israeli company NSO Group Technologies[14].

## II.1. THE PEGASUS CASE

20. The Pegasus software has become globally known for its stealthy installation and its potential to extract a large amount of data, both streaming and stored, from cell phones. **Its features and functionalities include the ability to access devices remotely, allowing the intruder to monitor and even control the device.**

**10** SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION. *Surveillance and Human Rights*. United Nations Human Rights. May 28th, 2018, p. 1

**11** FORMER UN SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION.

**12** Former member of the European Parliament and former director of the Cyber Policy Center at Stanford University.

**13** KAYE, D; SCHAAKE, M. Global spyware such as Pegasus is a threat to democracy. Here's how to stop it. *Washington Post*, July 19th, 2021. Available at: https://www.washingtonpost.com/opinions/2021/07/19/pegasus-spyware-nso-group-threatdemocracy-journalism/

**14** For more information, see the company's website: https://www.nsogroup.com.

21. Pegasus allows you to access and send messages, intercept, and make calls and video calls, turn your cell phone into a bug or a remote camera, and even access geolocation, i.e., record your mobility and track your device using GPS data[15].

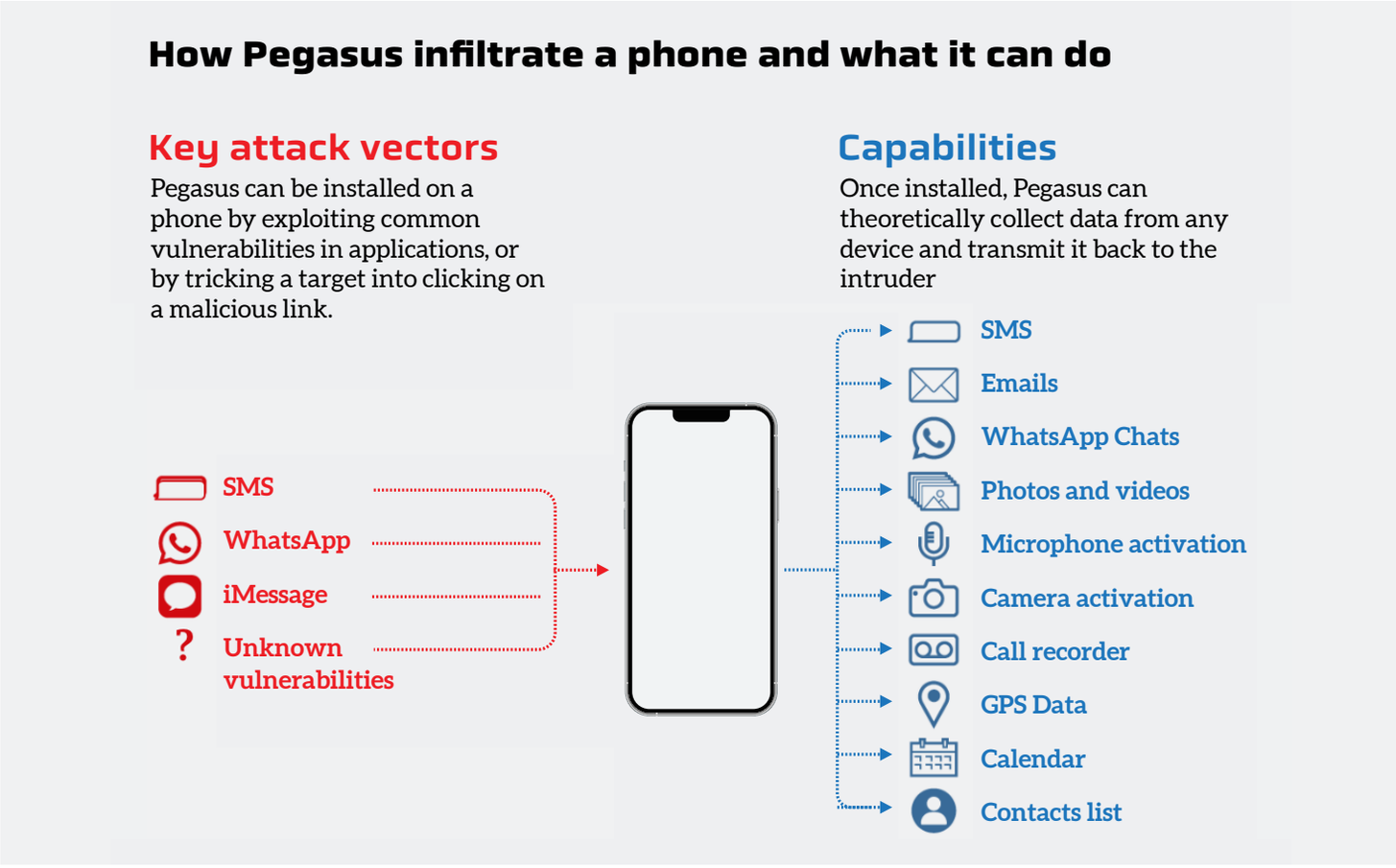


**Figure 1:** How Pegasus spyware works (The Guardian)[16].

22. In 2020, Forbidden Stories and Amnesty International published the leak of an NSO Group list with more than 50,000 cell phone numbers from more than 50 countries possibly targeted by NSO Group customers[17]. At the time, the Israeli company claimed that the leaked list was not theirs and that they were only selling it to governments to monitor the mobile devices of specific individuals suspected of being involved in serious crimes, such as "terrorism, pedophilia, sex, and drug-trafficking rings, kidnapping of children, among others"[18]. However, the

**15** PEGG, David, CUTLER, Sam. What is Pegasus spyware and how does it hack phones? *The Guardian*, July 18th, 2021. Available at: https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spywareand-how-does-it-hack-phones

**16** *Ibidem*

**17** FORBIDDEN STORIES. About the Pegasus Project, July 18th, 2021. Available at: https://forbiddenstories.org/about-the-pegasus-project/

**18** NSO GROUP. Enough is enough! Available at: https://www.nsogroup.com/Newses/enough-is-enough/

investigation found that "at least 180 journalists were targeted in countries such as India, Mexico, Hungary, Morocco, and France[19]. Along with journalists, "potential targets also include human rights defenders, academics, businesspeople, lawyers, doctors, diplomats, union leaders, politicians and several heads of states.[20]"

**23.** In the months following the release of the list, 17 media and science communication organizations and more than 80 journalists joined Forbidden Stories and Amnesty International, with the aim of revealing the illegitimate uses of Pegasus by governments.

**24.** In 2021, Amnesty International's Security Lab[21] published a report on the methodology and results of an "*in-depth forensic analysis of numerous mobile devices belonging to human rights defenders and journalists from around the world*"[22]. The report pointed to widespread use or intended use of Pegasus and identified profiles of monitoring targets, including academics, journalists, human rights activists, political representatives, and public officers[23].

**25.** In the years following the launch of the investigation, there were complaints and protests against the use of Pegasus. Non-governmental organizations and independent experts produced an open letter calling on states to implement an immediate suspension on the sale, transfer, and use of this type of technology. The Joint Open Letter[24] alerts us to the need to impose an immediate suspension on the sale, transfer, and use of surveillance technologies, given the risks to individual rights and freedoms.

**19** FORBIDDEN STORIES. About the Pegasus Project, July 18th, 2021. Available at: https://forbiddenstories.org/about-the-pegasus-project/

**20** *Ibidem.*

**21** The Amnesty International Security Lab is a multidisciplinary team of researchers, hackers, programmers, activists and advocates working to protect civil society from illegal digital surveillance, spyware and other human rights violations enabled by technology. More information: AMNESTY INTERNATIONAL. Security Lab - Homepage, 2024. Available at: https://securitylab.amnesty.org/.

**22** AMNESTY INTERNATIONAL. *Forensic Methodology Report: How to catch NSO Group's Pegasus.* July 18th, 2021. Available at: https://www.amnesty.org/en/latest/research/2021/07/forensic-methodologyreport-how-to-catch-nso-groups-pegasus/#_ftn1.

**23** FORBIDDEN STORIES. *Pegasus: the new global weapon for silencing journalists.* July 18th, 2021. Available at: https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/.

**24** The International Joint Open Letter in its original English version, can be found on the Transparency International website: https://www.amnesty.org/en/documents/doc10/4516/2021/en/.

**26.** The European Parliament also investigated the episode and produced a report[25], in which it argues that the lack of local regulations on the use of spyware, which prohibit the widespread use of these tools, has posed threats to human rights. It therefore argues that "the use of spyware should only be permitted **in exceptional cases** and for a limited period of time," and that:

> *spyware should only be used in Member States where allegations of abuse have been thoroughly investigated and national legislation complies with the recommendations of the Venice Commission and the case law of the Court of Justice of the EU, and export control regulations have been applied*[26].

**27.** However, NSO Group, the company responsible for manufacturing Pegasus spyware, **is just one of the many companies that make up the large private international market for remote surveillance and intrusion technologies**.

**28.** As Edward Snowden pointed out in an interview with *The Guardian*[27], such software does not provide any kind of protection for citizens, **but only forms of infiltration, i.e., violations of the right to privacy**[28].

**25** EUROPEAN PARLIAMENT. Investigation of the use of Pegasus and equivalent surveillance spyware. June 2013. Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747923/EPRS_ATA(2023)747923_EN.pdf.

**26** EUROPEAN PARLIAMENT. Spyware: MEPs call for full investigations and safeguards to prevent abuse. June 15th, 2023.

**27** Excerpts from the interview can be accessed here in the British Independent newspaper: PEGG, David; LEWIS, Paul. Edward Snowden calls for spyware trade ban amid Pegasus revelations. *The Guardian*, July 19th, 2015. Available at: https://www.theguardian.com/news/2021/jul/19/edward-snowden-callsspyware-trade-ban-pegasus-revelations?__twitter_impression=true.

**28** Excerpt from the interview: *"It's like an industry where the only thing they did was create custom variants of Covid to dodge vaccines," he said. "Their only products are infection vectors. They're not security products. They're not providing any kind of protection, any kind of prophylactic. They don't make vaccines – the only thing they sell is the virus."* cf. PEGG, David; LEWIS, Paul. Edward Snowden calls for spyware trade ban amid Pegasus revelations. *The Guardian*, 19 July 2015. Available at: https://www.theguardian.com/news/2021/jul/19/edwardsnowden-calls-spyware-trade-ban-pegasus-revelations?__twitter_impression=true

29. The Pegasus case is one example of many, and this should trigger an even greater alert. If the vulnerability exploitation industry purposely operates in an opaque manner, the consequence is that we have an environment in which there is a lack of knowledge and trust regarding the functionalities, capabilities, and levels of protection of human rights practiced in the provision of services by different companies.

30. However, a judgment on the fundamental rights affected by the different technologies offered by this industry needs to be based on a typology of these tools and their capabilities.

31. In the midst of technical expressions and different names, **the concrete effect that each functionality has on the user and on the integrity of the information system should be the parameter for understanding how these tools operate**. It is crucial to understand these differences in order to grasp the risk they pose.

32. For this reason, in the next topic we present **a typology of the different types of targeted surveillance tools (spyware) identified in Brazilian public administration contracts**, relating them to the degrees of risk that these tools present to fundamental rights. We seek to demonstrate, through the analysis of technologies used today, how the market for vulnerabilities in communications can affect the integrity of the information system, security in communications and trust in a democratic environment.

## II.2. THE VARYING DEFINITIONS AND FEATURES OF SPYWARES

33. Spywares are computer program with intrusive capabilities for extracting information and invading electronic and communications devices or systems, designed to exploit security flaws that may exist in these devices or in information networks and protocols through which communication flows. From an analytical point of view, spyware can be differentiated based on its *affordances* and possibilities for action.

**34.** Although rarely used in Brazilian constitutional law, the concept of *affordance* is widely used in contemporary computer law[29]. The concept of *affordance* was first developed in psychology and in studies on the environment and visual perception[30], and was later adopted in the areas of design and human-machine interaction[31]. *Affordances* concern the possibilities of action provided by a particular object or architecture.

**35.** Based on the discussion concerning *affordances* and potential for action, we analyzed how different architectures and code constructions produce certain types of possibilities for action, due to the characteristics of the computer programs themselves and their intentions. This differentiation allowed us to see more clearly different types of spyware, which can be differentiated functionally, producing precise descriptive categories.

**36.** The problem with considering all types of spyware as a monolithic, homogeneous block is that it reduces the complexity of this genre of computer programs, from which specificities arise. For this reason, the starting point is common characterizing elements, while presenting specific typologies.

**37.** Analytically, according to specialized literature[32], the different types of spyware need to go through **four common elements**, which make them identifiable as such:

> *(i) The data is obtained from a device by means of an extraction that* ***would not occur if it were not for the introduction of a computer program****, code, or attack;*
>
> *(ii) the data is extracted from the devices on the assumption that the user of the target device is not aware of* ***the extraction of information****;*

**29** HILDEBRANDT, Mireille. Law as Information in the Era of Data-Driven Agency. *The Modern Law Review*, v. 79, n. 1, p. 1-30, 2016. HILDEBRANDT, Mireille. Smart technologies. *Internet Policy Review*, v. 9, n. 4, p. 1-16, 2020.

**30** GIBSON, James J. *The ecological approach to visual perception*. Boston: Houghton Mifflin, 1979.

**31** MCGRENERE, Joanna; HO, Wayne. *Affordances*: Clarifying and evolving a concept. *Graphics interface*, 2000, p. 179-186.

**32** HARKIN, Diarmaid; MOLNAR, Adam; VOWLES, Erica. The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. Crime, media, culture, v. 16, n. 1, p. 33-60, 2020, p. 36-37.

*(iii)* ***the computer code or program is used in the context of creating a target****, whether an individual or a group of individuals, with the intention of monitoring, tracking and surveillance; and*

*(iv)* ***the data that is extracted from the devices has a specific legitimate context and can be considered private information****, such as location, photos, passwords, messages, application metadata, among others.*

**38.** For a better understanding and analysis of the software that is built to extract information from a user or system without the knowledge of the system owner or operator, we will systematically present the different capabilities of these tools.

**39.** **We have thus identified six (6) categories that can assist the Court in making a proper judgment on how the tools affect fundamental precepts:**

*1) Extraction on device;*

*2) Infrastructure extraction;*

*3) Cryptographic key compromise;*

*4) Extraction of deleted information;*

*5) Cloud communication system extraction;*

*6) Information extraction by inference*

**40.** Classification is not unique or exclusive, and therefore more than one software may comply with more than one extraction method. In fact, based on our analysis, we identified that **the vast majority of spyware has the ability to act in more than one way**, thus increasing its power to successfully invade the selected target.

41. **This proposed typology is applicable in practice.** Based on this categorization, we have classified the technologies listed in a research report on the technologies acquired by public authorities in the country. We have provided a map below, based on the Mercadores da Insegurança ("Merchants of Insecurity") report[33], indicating the spread of spyware in Brazil. In Doc. 01, we provide a chart containing its characteristics and classification based on the proposed typology.

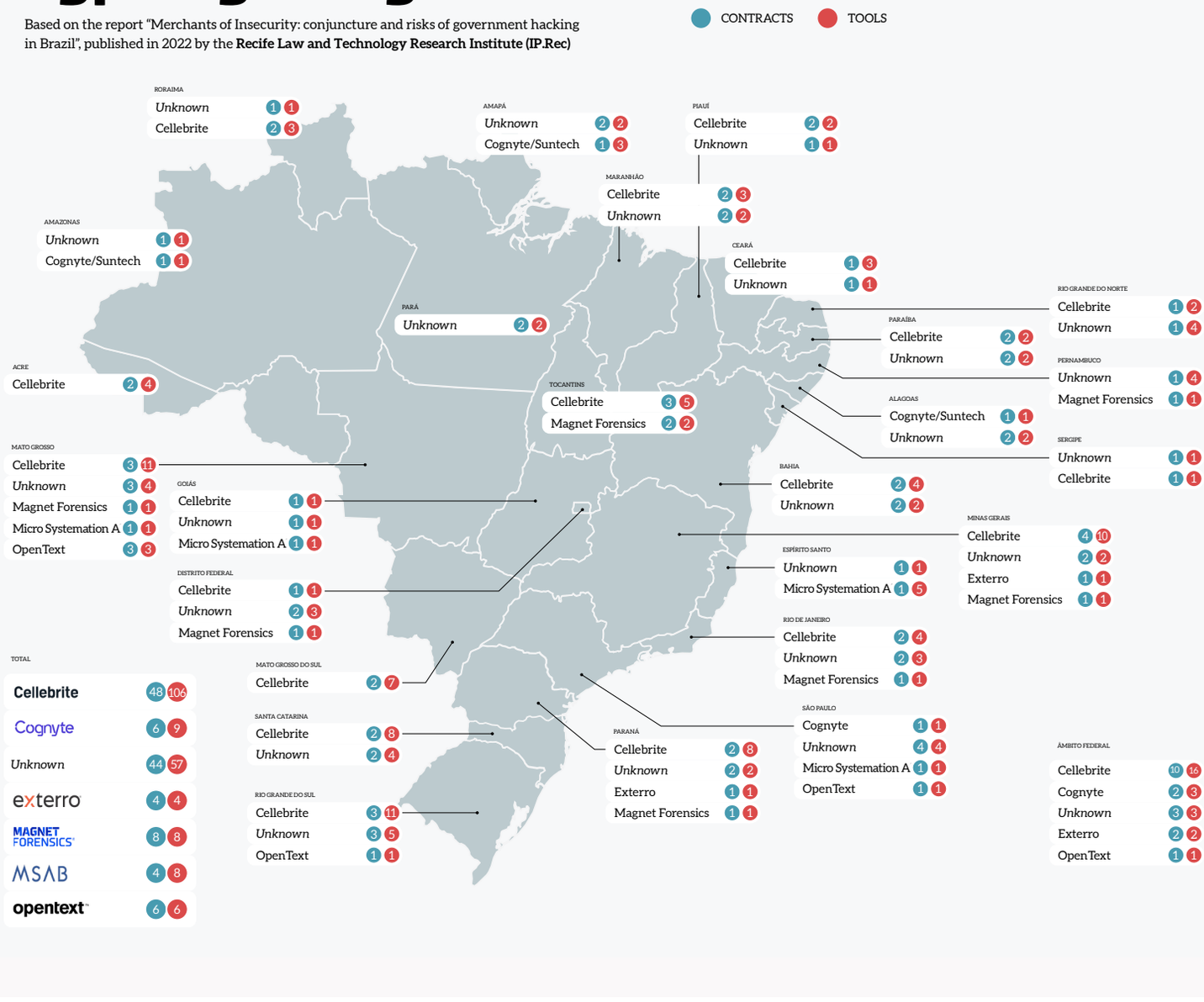


**Figure 2:** Typologies by state (Data Privacy Brasil)

33 AMARAL, P.; CANTO, M.; PEREIRA, M. C. M.; André Ramiro (coord.). *Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil*. Recife: IP.REC, 2022. Available at: https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf.

42. The purpose of constructing this typology is not only to provide an analytical gain from a descriptive point of view. We believe that, with a more accurate understanding of the different *affordances* of these types of spyware, the relationship between certain types of risks to fundamental rights becomes more evident and, in turn, requires a more robust institutional counterpart in the sense of creating control instruments, counterweights and institutional procedures capable of reducing the risks to citizens' fundamental rights.

43. Such threats to privacy rights are particularly sensitive, given that the right to privacy and the protection of personal data are foundational rights in democratic societies and enable the realization of other fundamental rights, such as the right to freedom of expression, the right to freedom of religion, the right to freedom of association, the right to due process, the right to freedom of movement, and the right to life and liberty. As recognized by Fionnuala Ní Aoláin, spyware affects fundamental rights in an interconnected way[34].

44. Spyware affects fundamental rights in a molecular (or interconnected) in that they are violated together and not in isolation, which represents a high-impact problem for the justice system in Brazil and for the proper protection of fundamental rights. The typology constructed allows us to consider the types of violations based on the possibilities of action (*affordances*), offering greater analytical clarity for an analysis from the perspective of constitutional rights and the effective protection of fundamental rights in Brazil.

### II.2.1. EXTRACTION ON DEVICE

45. Device extraction software are **tools capable of performing both logical and physical extraction on electronic devices**, which include cell phones, drones, SIM and SD cards, GPS devices, among others. This means they can extract all files or selected files from a device (such as social media files, messaging applications, or browsers), depending on the application used.

34 NÍ AOLÁIN, Fionnuala. *Global regulation of the counter-terrorism spyware technology trade: scoping proposals for a human-rights compliant approach*. Office of the High Commissioner for Human Rights. Geneva: United Nations, 2023, p. 34.

46. **This is the most common category among cyber intrusion tools used by the Brazilian government, accounting for more than half of the contracted software**. Some of these tools are: from the company Cellebrite, the models UFED, Physical Analyzer, Premium, Advanced Services and CHINEX; from the company Exterro/AccessData, the Forensic Toolkit; and from the company Micro Systemation AB, XRY Logical, Physical, Pinpoint (expansion), CRY Cloud and MSAB Office.

47. This category is the most commonly used by public security forces, investigative and forensic agencies in the context of an ongoing investigation. Device extraction tools are not necessarily used remotely, so the targeted device must be in the possession of the investigatigative authority.

48. As they require the physical presence of the electronic device, their targets, at least in theory, know that they have been subjected to search and seizure procedures. However, the physical need for the electronic device does not diminish the seriousness of the access to private communications. It is, in any case, the possibility of breaking the secrecy of private communications that requires compliance with the formal rites of due process of law, as well as observance of the fundamental procedural guarantees of the individuals under suspicion.

49. Direct investigative procedures on the device can also pose risks of speculative search (fishing expedition)[35] that lack a defined purpose and exceed reasonable limits, or the risk of accessing personal files that have no relation to the ongoing investigation.

50. Although they cannot be directly treated as "remote intrusion tools," regulating the use of this category would minimally bring legal certainty to the chain of custody process and the ordering of investigations on national territory.

35 SILVA. Viviani Ghizoni da; MELO E SILVA, Philipe Benoni; ROSA, Alexandre Morais da. *Fishing Expedition and Fortuitous Encounter in Search and Seizure. Florianópolis: Emais Editora & Livraria Jurídica, 2nd Edition, 2022.*

## II.2.2. INFRASTRUCTURE EXTRACTION

**51.** Infrastructure extraction software are **tools capable of performing extraction by infiltrating public or private network infrastructures**.

**52.** This infiltration can occur through flaws in system protocols that should be shared only between telecommunications operators, or through security vulnerabilities in the system. It can take developers months to fix these errors and breaches. There are also situations in which telecom operators are neglectful, such as the flaw exploited by FirstMile, which has been known about for years[36] [37].

**53.** Examples of this category are the FirstMile, GI2 and PI2 tools, operated by the company Cognyte[38]. **FirstMile**, whose use by the Brazilian Intelligence Agency (Abin) has been investigated by the Federal Police, was allegedly used to monitor authorities, journalists, activists, and ministers of the Brazilian Supreme Court (STF)[39].

**54.** The tool is capable of accurately identifying the location of electronic devices using the 2G, 3G and 4G networks. This occurs through flaws in the Signaling System No. 7 (SS7) protocol, a phenomenon already identified by the computer science community more than ten years ago. SS7 is a protocol that allows different operators to communicate and share information, such as monitoring the position of devices, to guarantee the delivery of SMS messages.

**36** KURTZ, João. *Cell phone network flaw leaves gap for banking attacks.* Techtudo. May 10th, 2017. Available at: https://www.techtudo.com.br/noticias/2017/05/falha-em-rede-de-celulares-deixa-brecha-para-ataques-bancarios-entenda.ghtml.

**37** In 2017, the organization CodingRights demonstrated how information security researchers had been warning about the vulnerabilities, cf. TEIXEIRA, Lucas. *Consulting the pocket spy: SS7 vulnerabilities and global tracking*. Medium, July 28th, 2017. Available at: https://medium.com/codingrights/consultando-o-espi%C3%A3o-de-bolso-vulnerabilidades-ss7-e-rastreamento-global-bc9920008c3c.

**38** In 2021, Verint created a company called "Cognyte", derived from the Cyber Intelligence sector focused on business solutions. More information at: https://www.verint.com/press-room/2021-press-releases/verint-celebrates-day-one-as-a-company-focused-on-enabling-brands-to-achieve-boundless-customer-engagement-following-completion-of-cognyte-software-spin-off/ & https://www.businesswire.com/news/home/20210622005107/en/Cognyte-Starts-as-a-Separate-Public-Company-with-Strong-First-Quarter-Results

**39** WHAT is FirstMile, the software allegedly used by Abin to monitor journalists and STF justices. Correio Brasiliense, Jan. 25, 2024. Available at: https://www.correiobraziliense.com.br/mundo/2024/01/6792403-o-que-e-o-firstmile-software-que-teria-sido-usado-pela-abin-para-monitorar-jornalistas-e-ministros-do-stf.html

55. FirstMile, based on a *spoofing* technique that emulates communications that should be genuine between devices that operate on the basis of this communication protocol, can monitor up to 10,000 cell phone owners every 12 months, just from the desired telephone contact number.

56. In addition, the system is capable of generating alerts on the routine movement of targets of interest. Although it is not as precise as GPS, the aggregation of location information in a base station (ERB) allows the identification of location patterns and intensifies threats to individual freedoms.

57. The GI2 is able to locate the target device precisely, using a dedicated homing device, without disabling the target from communicating; extract the GPS coordinates of the target's cell phone on GSM and UMTS (3G) networks; listen to, read, edit, and redirect incoming and outgoing calls, as well as text messages (A5/1 and A5/3 encryption); remotely activate the microphone of a cell phone; Identify the presence of the target's handset; block cellular communications to neutralize IEDs and intercept incoming and outgoing SMS.

58. PI2, on the other hand, is capable of collecting GSM traffic in a "broad range", as well as intercepting calls and text messages, breaking encryption, analyzing "suspicious communication patterns" and allowing multiple users to analyze calls at the same time.

### II.2.3. CRYPTOGRAPHIC KEY COMPROMISE

59. **Software for Cryptographic Key Compromise are tools capable of bypassing the security mechanisms of a device, breaking the encrypted passwords needed to access the device**. This can occur, for example, through the unlocking of devices protected by patterns, passwords, or PIN codes, as well as bypassing encryption on Android and iOS devices.

60. Cryptography is, broadly speaking, a resource that protects the security of information by using mathematical techniques to encode and decode it, which is fundamental to ensuring the availability, integrity, and confidentiality of any data exchanges and communications on the internet. As shown in section III.2, the justices of this esteemed court have already indicated that cryptography is a security mechanism that promotes fundamental rights[40].

61. In case of strong cryptography, no one other than the parties involved can access the data sent or received, not even the provider of the device or communication channel. However, security vulnerabilities in the protocols developed can be found and exploited by the companies developing these tools, making the content of the communications accessible and violating confidentiality.

62. **In general, these software tools are purchased along with other tools that include intrusive features**. Among the analyzed software, Encase Forensic[41] from OpenText is the specialist tool in this category, with access to data encrypted with BitLocker (Windows 10), Data Protection 8.17 (Dell), and PGP v10.3 (Symantec), as well as access to data encrypted with APFS (Apple File System) and bypassing security for the Apple T2 Security.

### II.2.4. EXTRACTION OF DELETED INFORMATION

63. **This category includes tools capable of recovering deleted files from an electronic device**. They enable the retrieval of documents from the device itself or even data from other applications such as WhatsApp, Facebook, and Telegram, as well as access to emails and attached files.

40 In the Direct Action for the Declaration of Unconstitutionality (ADI) nº 5.527 and in the Action Against the Violation of a Constitutional Fundamental Right (ADPF) nº 403, the Supreme Court recognized the importance of privacy in digital media, stating that the creation of backdoors (the creation of exceptional means to access encrypted user data) creates mass security breaches, ruling that the adoption of end-to-end encryption in internet applications is constitutional. This matter will be further developed in this petition.

41 Details of the product available at: https://www.opentext.com/pt-br/produtos/encase-forensic.

64. This functionality can be found in Cellebrite's UFED and Physical Analyzer software, Exterro/AccessData's Forensic Toolkit and Micro Systemation AB's XRY Physical and MSAB Office. 65.

### II.2.5. CLOUD COMMUNICATION SYSTEM EXTRACTION

65. **Cloud communication system extraction spywares are tools capable of extracting data from applications with cloud storage, such as Facebook, Google, iCloud, Twitter, and Snapchat**. This includes automatic extraction, using access tokens from applications previously extracted with the device in hand, and manual extraction, without the need for the device to be present, using login and password previously accessed through other means. It can be found in the UFED Cloud (Cellebrite), Magnet AXIOM (OpenText) and CRY Cloud (Micro Systemation AB) tools.

### II.2.6. INFORMATION EXTRACTION BY INFERENCE

66. **Information extraction by inference spywares are highly invasive tools capable of processing data to generate "new" information through complex analyses of the devices.**

67. This type of functionality includes the analysis, filtering, visualization, and systematization of data extracted from mobile devices, drones, wearable technologies, GPS, vehicles, SIM cards, and the recognition of content in images, memory cards, and other sources. It also involves the unification of databases for evidence storage with indexing, filtering, and search tools for querying stored data results.

68. Examples include UFED Cloud, Pathfinder, and Commander software from Cellebrite; Magnet AXIOM from OpenText; Forensic Toolkit from Exterro/AccessData; and XAMN Horizon and XAMN Spotlight from Micro Systemation AB.

**69.** This category represents more sophisticated software, which are more complex tools that use Open Source Intelligence (OSINT) mechanisms and/or artificial intelligence for data exploration and analysis. This characteristic demonstrates a potential for growth, keeping pace with the advancement and expansion of artificial intelligence

**70.** These spywares introduce an additional layer of intelligence, capable of linking associations and locations of individuals and making correlations and inferences in a non-transparent manner. This lack of transparency can lead to misinterpretations in information analysis, for example, by reproducing biases already seen in various new tools that use facial recognition technologies and artificial intelligence[42]. Furthermore, due to their extremely opaque nature, their biases can be reproduced in investigative and intelligence activities, creating widespread risks to individuals and social groups subjected to these spywares.

## II.3. THE NECESSARY DIFFERENTIATION BETWEEN SPYWARES AND OPEN SOURCE INTELLIGENCE (OSINT)

**71.** Given the characteristics and types of spywares, it is necessary to explain what OSINT is and thus differentiate this technology from spyware tools. Open Source Intelligence (OSINT) is an intelligence service that operates through public data and open sources such as social media, media outlets, blogs, tweets, and news.

**72.** According to Koops, Heopman, and Leenes (2013)[43], open source intelligence (OSINT) is a process of collecting, analyzing, and using data from open sources for intelligence purposes. Howells and Ertugan (2017)[44], **define OSINT as a**

**42** The article 'Insufficiency of ethical principles for the standardization of Artificial Intelligence: anti-racism and anti-discrimination as vectors of AI regulation in Brazil' demonstrates the problem of using AI without regulation based on human rights. Available at: https://www.dataprivacybr.org/documentos/insuficiencia-dos-principios-eticos-para-normatizacao-da-inteligencia-artificial-o-antirracismo-e-a-anti-discriminacao-como-vetores-da-regulacao-de-ia-no-brasil/?idProject=2331

**43** KOOPS, Bert-Jaap; HOEPMAN, Jaap; LEENES, Ronald. Open-source intelligence and privacy by design. Computer Law & Security Review. *Computer Lay and Security Review*, v. 29, n. 6, p. 676-688, 2013. Available at: https://www.cs.ru.nl/J.H.Hoepman/publications/osint-pbd.pdf

**44** HOWELLS, Karen; ERTUGAN, Ahmet. Applying fuzzy logic for sentiment analysis of social media network data in marketing. *Procedia Computer Science*, v. 120, p. 664-670. 2017. Available at: https://www.sciencedirect.com/science/article/pii/S187705091732505X

**method of intelligence collection management that locates, selects, and extracts information from open sources, such as Twitter and Facebook, and then analyzes the information to produce intelligence**. In the field of information security, this data collection process aims to produce current and relevant information that is valuable to an attacker or a competitor.

73. Thus, the **main difference between spywares and OSINT is the way they obtain data:** the former exploit vulnerabilities in code and software programs to access users' data without their consent. **The OSINTs, on the other hand, uses public data sources available on the World Wide Web to create intelligence through the compilation, systematization, and interpretation of open sources.**

74. Therefore, the two technologies are distinct methods of making inferences and collecting evidence about people and institutions. Although both operate without users' consent, spywares invade systems, collecting data that is often confidential and restricted.

75. Differentiating these technologies is essential to the debate, as **OSINT, despite potential arbitrary uses, can also be employed in contexts that promote fundamental rights.** It is also noteworthy that investigative journalism uses OSINTs lawfully, creating effective mechanisms for fact-finding

76. Despite the positive use of this technology, we emphasize the need for regulation and control of its use by the state. The use of these tools for extensive collection of dispersed information in the digital realm, which can detect, analyze, and produce reports detailing connections, goes beyond merely focusing on criminal activities and extends, alarmingly, to the monitoring and profiling of activities that represent a free exercise of civil and political rights.

77. In the following section, we indicate how these multiple functionalities are presented based on facts.

### II.3.1. OSINT, HARPIA TECH, AND THE OVERREACH OF THE STATE'S INTELLIGENCE CAPABILITIES

**78.** On May 19, 2021, the Ministry of Justice and Public Security launched Bid Notice No. 03/2021[45], in the electronic procurement modality, aiming to meet the operational needs of the Intelligence Directorate of the Secretariat of Integrated Operations (SEOPI). The purpose of the bid was to acquire a "Solution for Open Source Intelligence, Social Media, Deep and Dark Web"[46].

**79.** The motivation was tied to the restructuring of the Public Security and Intelligence Subsystem[47], aiming to enhance the analytical capabilities of intelligence professionals, as well as to enable a more qualified exchange of information among them. The winning company, Harpia Tecnologia Eireli (Harpia Tech), offered a bid of R$ 5,415,750.00 (five million, four hundred and fifteen thousand, seven hundred and fifty reais[48] for the collection of information from open sources, returning more than 15,000 results per search, such as social media posts, Dark Web, emails, contact phone numbers, demographic information, among others[49]. Additionally, the tool allows the classification of "*[...] people, groups, companies, organizations, web pages, internet infrastructure, phrases, documents, files, among others*," as well as the ability to visualize all this information in the form of reports.

**80.** To clarify: "*[...] the tool generates an intelligence report with different perspectives on the information collected. The items in the report can also be customized*"[50].

**45** Advertisement for bids N. 03/202; Electronic Procurement N. 3/2021; Case N. 08000.000865/2020-30. Available at: https://www.gov.br/mj/pt-br/acesso-a-informacao/licitacoes-e-contratosv1/licitacoese-contratos-segen/cglic/cpl/procedimentos-2021/pregao-2-2021-1/edital_completo.pdf.

**46** "The purpose of this bidding process is to select the most advantageous proposal for the acquisition of an Open Source Intelligence Solution, covering Social Media, Deep, and Dark Web, including supply, installation, configuration, and technical support, in order to meet the operational needs of the Intelligence Directorate of the Secretariat of Integrated Operations (DINT/SEOPI)", Bidding Notice N. 03/202 p. 01.

**47** Meeting the equipment needs of the Central Agency of the Intelligence Subsystem, integrating with other Public Security Intelligence Agencies (PSIA), and fulfilling the strategic objectives of the Ministry of Justice and Public Security. Bidding Notice N. 03/202 p. 24.

**48** Ministry of Justice and Public Security. Result of the Judgment of the Bidding Process N. 3/202, Published in the Federal Gazette (DOU), Section 3, No. 152, Thursday, August 12, 2021. Available at: https://www.gov.br/mj/ptbr/acesso-a-informacao/licitacoes-e-contratosv1/licitacoes-e-contratossegen/cglic/cpl/procedimentos-2021/pregao-2-2021-1/resultado_de_julgamento___dou-pe-3.pdf.

**49** Administrative Process nº 08000.000865/2020-30.

**50** Administrative Process nº 08000.000865/2020-30, p. 6.

**81.** Because it is a solution that collects digital data, aggregating and cross-referencing this information to develop profiles of individuals for intelligence purposes, **its use opens the door to the continuous production of profiles and the ongoing monitoring of anything that Intelligence classifies as a threat**[51].

**82.** It is therefore fair to say that the collection of information from these different sources results in a **digital dossier** of the person(s) being investigated, which allows for the composition of this analytical scenario. Although it is not a dossier in the classic sense[52], the software's ability to aggregate and integrate disaggregated data in real time, producing knowledge about the desired target, generates a dossier in the literal sense of the term: a collection of information about an individual, group or organization.

**83.** Similar to spywares, which are the focus of this statement, the spread of surveillance technologies such as OSINTs (Open Source Intelligence), without adequate safeguards and proportionality tests against the violation of fundamental rights, **represents a violation of rights that is incompatible with the Democratic Rule of Law and constitutional rights.**

**51** Examples provided by Harpia when describing the solution's functionalities: "In the example below, the mention of a Federal Police IP by a malicious actor triggers the data collection process from an IRC messaging service group. The organization is duly categorized. By clicking on the link next to the entity's name, the user receives all search history results related to the entity. **The author of the publication is also cataloged, and clicking on their name redirects the user to a specific analysis screen about the individual, which includes a timeline and link analysis";** "In the screen below, **we present actors systematically monitored by the tool:** [...] In the virtual presence column, it is possible to see **the different networks and platforms on which each individual is monitored** (examples: Twitter, Reddit, Facebook, YouTube, GitHub, Discord...);" and "Analysis screen of a Brazilian criminal. On the screen above, **in addition to the timeline, it is possible to view link analyses ('mentioned' items and 'relationships between actors'), the different media in which the criminal's presence is observed** (in this case, Twitter, Facebook, YouTube, Skype, Zone-H, and GitHub), **the classification of their status, affiliation with a particular group, as well as other relevant information.**" (our emphasis)

**52** As in the case of the old records produced by DOI-CODI during the dictatorship, for example, being massively used by the National Truth Commission in the investigation of human rights violations during the civil-military dictatorship. See ZANATTA, Rafael. *The Collective Protection of Personal Data in Brazil: Interpretation Vectors*. Belo Horizonte: Letramento, 2023.

**84.** As argued by Steven Feldman, these computer programs organized as OSINTS for surveillance are capable of not only aggregating thousands of data points into a single analysis dashboard, but they can also apply Artificial Intelligence techniques for inferential analysis of profiles and suspicious conduct[53]. Even if it's not the same as the NSO Group's Pegasus, the potential uses in violation of fundamental rights cannot be ignored, especially when targeting and persistent profiling techniques are used on a person.

### II.3.2. THE OSINTS POTENTIAL FOR PROMOTING HUMAN RIGHTS AND JOURNALISM

**85.** Among the uses of OSINTs that promote fundamental rights and public goods, we can mention their role in journalism. It has become a widespread method among journalists, activists, and the UN system[54], enabling collaborative checks, through open data intelligence, to identify human rights violations.

**86.** According to researchers Michael Glassman and Min Ju Kang[55], an OSINT is not a new type of intelligence, but has generally emerged in human problem-solving during specific types of object-oriented activities. Its practice is seen in a positive light, particularly as a conventional data collection method that does not violate human rights[56]. Some examples are listed below.

**87.** *Bellingcat*[57] is an investigative journalism group based in the Netherlands, specializing in fact-checking through OSINTs. *Bellingcat* publishes reports on war zones, human rights violations, and the criminal underworld. The

**53** FELDSTEIN, Steven. *The global expansion of AI surveillance.* Washington, DC: Carnegie Endowment for International Peace, 2019.

**54** The UN uses OSINTs, for example, to combat trafficking in synthetic drugs, even offering free training and tools to member states. Available at: https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/investigation/OSINT.html.

**55** GLASSMAN, MICHAEL; KANG, MIN JU. Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). Computers in Human Behavior, v. 28, n. 2, p. 673-682, 2012. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0747563211002585.

**56** HRIBAR, GAŠPER; PODBREGAR, IZTOK; IVANUŠA, TEODORA. OSINT: a "grey zone"? International Journal of Intelligence and Counterintelligence, v. 27, n. 3, p. 529-549, 2014. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0747563211002585.

**57** https://www.bellingcat.com

organization has investigated, for example, the execution of people by cartels in Mexico[58] and murders during the Syrian War[59]. The *Ceasefire Centre for Civilian*[60] monitors potential violations of international humanitarian law and human rights in a decentralized manner using OSINTs. An example is the case of human rights violations against the Yazidi and Alawite minorities after the invasion of northern Syria[61].

**88.** In Brazil we have *Territórios de Exceção* (Territories of Exception)[62], a research initiative on the police use of helicopters as a firing platform in densely populated regions, especially in favelas, particularly in the Maré Complex in Rio de Janeiro. Using OSINTs, the research identified patterns in the use of this military apparatus in the city during 2018 and 2019, identifying 415 operations using helicopters, and in at least 60 of them there was evidence of the use of aircraft as a firing platform.

**89.** Finally, *Amazônia Minada* (Mined Amazon)[63] shows the mining processes in the Brazilian Amazon, obtained from public data from the National Mining Agency (ANM), mapping and alerting when mining processes overlap (totally or partially) or are adjacent to indigenous lands and integral conservation units in the Legal Amazon, crossing open data from the National Mining Agency, Funai, Ministry of the Environment and InfoAmazonia.

**90.** The highlights above are intended to emphasize the importance of the conceptual separation between OSINTs and spyware, pinpointing the use of the former with its potential to both violate and promote human rights. In this scenario, safeguards and proportionality tests can guarantee the lawful

**58** COUNTERING the Cartel: Darktrace's Investigation into CyberCartel Attacks Targeting Latin America. Darktrace. 8 Jan. 2024. Available at: https://darktrace.com/blog/countering-the-cartel-darktraces-investigation-into-cybercartel-attacks-targeting-latin-america.

**59** INSIDE SJAC's Open-Source Investigative Team. *Syria Justice and Accountability Centre*.16 Nov. 2022. Available at: https://syriaaccountability.org/inside-sjacs-open-source-investigative-team/.

**60** For more information: https://www.ceasefire.org/.

**61** CEASEFIRE. The Yazidi Survivors' Law: A step towards reparations for the ISIS conflict. [S.D.] Available at: https://www.ceasefire.org/wp-content/uploads/2021/05/Yazidi-Survivors-Law-Briefing-1.pdf.

**62** MEDIALAB.UFRJ; AGÊNCIA AUTÔNOMA. *Territórios de Exceção:* Rights violation and the use of police helicopters in Rio de Janeiro. 2021. Available at: https://documental.xyz/pt/intervencao

**63** INFOAMAZONIA. Amazônia Minada. 2022. Available at: https://minada.infoamazonia.org/

use of OSINTs. On the other hand, spyware deserves greater attention from law enforcers, due to its high degree of invasion and possible violation of the fundamental rights of individuals who are victims of these tools.

## III. THE USE OF SPYWARES IN LIGHT OF FUNDAMENTAL RIGHTS

**91.** After analyzing what these programs entail, **it is necessary to clarify what the violation of a fundamental precept, as examined by this Honorable Court, means:** it involves ultimately **allowing the use of extremely invasive technological tools by state agencies and intelligence service. Even more concerning is that these tools have, as a corollary, the buying and selling of information security vulnerabilities of all citizens, precisely due to how this market is structured.**

**92.** As a result, fundamental rights are placed under serious threat of violation, such as the rights to privacy, security of communications, image, location, among others.

**93.** In recent years, the debate on how spyware affects fundamental rights has intensified, drawing important analysis from the international human rights system. The UN special rapporteur on counterterrorism, Fionnuala Ní Aoláin, has stated that the various cases already documented in Saudi Arabia, Sudan, Iraq and countries with documentation of people affected by spyware point to situations of multiple violations of international human rights standards, such as the right to life, unlawful exposure to violence, unjust imprisonment, disproportionate interference with the right to privacy, disproportionate interference with the rights to freedom of expression, freedom of association and freedom of religion[64].

**94.** It is clear that the operation of this industry, under the pretext of combating serious crimes such as terrorism, generically affects the fundamental rights of individuals without any express justification provided by law or other limits

64 NÍ AOLÁIN, Fionnuala. Global regulation of the counter-terrorism spyware technology trade: scoping proposals for a human-rights compliant approach. Office of the High Commissioner for Human Rights. Geneva: United Nations, 2023, p. 22-23.

that examine the proportionality of the use of these tools. The unrestricted and unregulated use of many of these technological tools authorizes the government to arbitrarily investigate any citizen's data in search of hypothetical illegalities. It is, therefore, an exercise in trial and error, whereby **users have their privacy stripped away and become targets of coercive measures** simply because there is some kind of suspicion, even if minimal, about them.

95. Indeed, **the absence of regulation ultimately means unrestricted permission** since there are no parameters to follow when using these tools or an express legal prohibition. This allows for an unjustifiable "fishing expedition" of unsuspecting people for criminal investigation, conducted covertly, without those affected having the opportunity to defend themselves, since these invasion technologies take place without the individual even being aware of them at any time.

96. Allowing the investigative authority unrestricted access to data on those being investigated opens the door to abuses of power. There is also the risk of establishing a police state, in which cell phones and all the applications on them are transformed into surveillance tools, in violation of civil liberties. It is a question of thwarting the individual guarantees provided for in the Constitution and which are given the status of fundamental rights.

97. **Consequently, in this contribution we argue that the state has a duty to refrain from buying or in any way acquiring remote intrusion technologies, which seriously threaten the democratic state and the right of all citizens to privacy and freedom of expression.**

98. **To this end, we defend the existence of a right to the integrity of information systems**, which stems from the constitutional protections already guaranteed to privacy and data protection and repeatedly reinforced at different times by this Court, and which compel public administration bodies to act in such a way as to protect - and not make vulnerable - the security of their citizens' communications.

99. Finally, we will primarily defend **the lack of proportionality and necessity in the use of remote intrusion technologies,** considering the degree of intrusiveness and risk of such measures in relation to their potential benefits for criminal investigations.

**100.** Nevertheless, in the alternative, in cases where it is necessary to use spyware tools, as the only possible measure for criminal prosecution, the Brazilian authorities must pay attention to strict observance of the necessity and appropriateness of the measure in specific cases, with strict criteria and treatment analogous to the existing regulations for other cases of breach of confidentiality, as well as regulations on the chain of custody of evidence, which is even more important due to the very characteristics of intrusive mechanisms.

**101.** The following sections of this contribution will focus on the arguments listed above.

## III.1. THE DEMOCRATIC IMPACT OF VULNERABILITY EXPLOITATIONS

**102.** By purchasing, acquiring, or otherwise using spyware tools, **state bodies exploit an industry that creates vulnerabilities in the communications and information systems of all their citizens.**

**103.** **Such vulnerabilities compromise the security of users and the entire chain of use of the communications infrastructure.** This also includes productive and essential sectors of the economy such as financial[65] and health companies[66], where the need for security in information traffic and secrecy regarding the content transmitted is of key importance for the reliable existence of the market.

**104.** The failure to repair a vulnerability in the system not only affects a person who is being investigated, **but the entire production system that relies on these infrastructures to conduct its operations.**

**65** CALLIESS, Christian; BAUMGARTEN, Ansgar. Cybersecurity in the EU the example of the financial sector: a legal perspective. *German Law Journal*, v. 21, n. 6, p. 1149-1179, 2020. Available at: https://www.cambridge.org/core/journals/german-law-journal/article/cybersecurity-in-the-eu-theexample-of-the-financial-sector-a-legal-perspective/E74D7AB0D2FDF2B0017BD93BD324267C.

**66** KRUSE, Clemens Scott et al. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, v. 25, n. 1, p. 1-10, 2017. Available at: https://content.iospress.com/articles/technology-and-health-care/thc1263.

**105.** Naturally, **faced with a normative-institutional scenario in which vulnerabilities not only exist, but are encouraged by the state - through repeated financial incentives to the country - the quality of public debate and trust in democratic institutions is also affected.** Firstly, because of the possibility of uses by public officials that escape the limits of legality, ethics, and proportionality. Secondly, not only because of the factual and material possibility of abuses within the public administration, but also because of the possible *inhibiting effects* that the use of technologies like these can have on freedom of expression.

**106.** The recent cases in Brazil that were mentioned earlier highlight the first possibility. **They show that state agents can corrupt their functional activities and use these tools for their own benefit.**

**107.** **These cases illustrate how the state's surveillance apparatus, when not severely limited and subject to strict rules, can be distorted.** Instead of serving lawful institutional purposes, such as addressing serious crimes, it can be used for individual and political objectives that threaten the democratic rule of law and the principles of impersonality and legality in public administration.

**108.** On the other hand, **the legitimization of targeted monitoring tools imposes an environment of distrust in democratic institutions.**

**109.** **In this respect, privacy and freedom of expression are directly related.** State surveillance that emerges without control or justification has harmful impacts on human behavior, influencing the way individuals interact in society and even their psychological state. As Alan Westin argues, privacy has social and political relevance, and is a crucial component of democratic systems[67]. The absence of privacy, in turn, results in harmful effects on individual autonomy, politics, decision-making and opinion. Ensuring the preservation of the right to privacy of all citizens is therefore a primary responsibility of the Democratic State of Law and should serve as a guiding principle for all state activities that involve the collection and processing of data.

**67** WESTIN, A. F. *Privacy and freedom*. New York: Ig Publishing, 2015, p. 246

**110.** Accordingly, **the inhibiting effects of the State's surveillance capabilities on freedom of expression have been widely studied and evidenced.**

**111.** This Court has already ruled that within the right to freedom of expression is "*the ability of individuals to freely choose the information they wish to share, the ideas they wish to discuss, the style of language employed and the means of communication*"[68]. However, in an environment of constant risk and fear that communication will be monitored by third parties, "citizens may change the way they express themselves or even refrain from speaking about certain subjects" [69].

**112.** This phenomenon has become known for the *chilling effects* that state measures can have on the expression of the entire community, including citizens who have not yet been the target of surveillance. Its consequences range "*from distrust of social institutions to generalized apathy and the weakening of intellectual life, creating an environment in which communication activities are inhibited or timid*"[70]. The existence of spyware in state bodies produces an intimidating environment for communication, which in itself damages the freedom of expression of thousands of citizens.

**113.** This applies not only when a person knows that he or she is being watched, but also when a person knows that *there is a possibility that he or she will be under surveillance*, without ever knowing for sure when this will happen. According to jurist Daniel Solove:

> *A more compelling reason why covert surveillance is problematic is that it can have an intimidating effect on behavior. In fact, there can be an even more intimidating effect when people are generally aware of the possibility of surveillance but are never sure if they are being watched at any particular time. [...] Thus, awareness of the possibility of surveillance can be just as inhibiting as actual surveillance*[71].

**68** BRAZIL. Brazilian Supreme Court. Direct Action for the Declaration of Unconstitutionality (ADI) No. 5.527. Vote by Justice Rosa Weber, p.36. Available at: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf.

**69** *Ibidem*, p. 10.

**70** *Ibidem*, p. 11.

**71** SOLOVE, Daniel J. A taxonomy of privacy. *University of Pennsylvania Law Review*, v. 154, n. 3, Jan. 2006, p. 494-495.

**114.** The current scenario envisages the possibility of purchasing and using targeted surveillance tools, which operate without the target having any knowledge of the remote monitoring or the ability to defend themselves. **The absence of clear legal parameters and specific criteria to guide the activities of public authorities makes the ability to use these tools absolutely discretionary.**

**115.** Although defense and intelligence agencies have regulations regarding their activities and councils that, at least in theory, oversee the agency's activities, what we see in practice is the absence of normative-institutional parameters that provide guidelines for their investigative capabilities[72].

**116.** On the other hand, a generic permission to purchase and use such tools covers not only the Federal Government and Abin, but also other entities, such as states and municipalities, which have an interest in acquiring them. In these cases, the limits and attention to the parameters of legality and reasonableness become even more unclear[73].

**117.** **Insofar as this scenario unfolds and is upheld on a daily basis, the democratic environment is already affected.** Political activists, journalists, academics, teachers and members of collectives or social movements tend to remain in a state of continuous suspicion. The reason for this is that they never know when, if and under what conditions they may be under surveillance by political opponents who hold public office at the most diverse levels of the federation.

**118.** Freedom of opinion, association, and expression, in this scenario, is constantly at the mercy of the changing political forces. **This creates an environment of collective insecurity and distrust in public security and defense institutions, which is harmful to any modern democracy that is also dependent on these institutions for its continuity.**

**72** INTERNETLAB. *The law of digital investigations in Brazil: foundations and regulatory frameworks*. São Paulo: InternetLab, 2022. Available at: https://internetlab.org.br/wpcontent/uploads/2022/10/INTERNETLAB_O-DIREITO-DAS-INVESTIGACOES_PRINT_10-2022.pdf.

**73** AMARAL, P.; CANTO, M.; PEREIRA, M. C. M.; André Ramiro (coord.). *Merchants of insecurity: the situation and risks of government hacking in Brazil*. November 2022. Available at: https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf.

**119.** The repeated use of spyware tools by state authorities, therefore, implies harmful consequences for the democratic environment, whether (i) due to the impact this has on the telecommunications infrastructure's security, (ii) due to the inhibiting impact on freedom of expression and the population's trust in institutions, or (iii) due to the possibility of such tools being easily used for anti-democratic purposes, which are contrary to the principles of legality and impersonality in public administration, as several cases have already pointed out in Brazil and around the world.

**120.** The above result requires us to consider the **State's duty to protect the informational environment by (i) not using remote intrusion tools on electronic systems; (ii) recognizing the illegality of acquiring these tools; and, finally, (iii) encouraging vulnerability disclosure policies.**

**121.** These consequences **reinforce the need to defend the right to the integrity of informational systems,** which stems directly from the constitutional protections guaranteed for privacy, data protection, and informational self-determination, all of which are crucial for maintaining our democratic environment. It is imperative to recognize a right to the integrity of informational systems as a component of the Brazilian constitutional tradition of protecting human dignity in a Democratic State of Law, considering that informational self-determination is a component of personality rights, as already decided by this Supreme Court. In this sense, the right to the integrity of informational systems is recognized as an extension of the constitutional interpretation of the right to personal data protection, connected to the clauses ensuring freedom and human dignity[74].

## III.2. THE FUNDAMENTAL RIGHTS TO CONFIDENTIALITY OF COMMUNICATIONS AND TO PERSONAL DATA PROTECTION

**122.** The Federal Constitution protects the rights to intimacy, privacy, confidentiality, and personal data protection (Article 5, X, XII, and LXXIX).

**74** MENKE, Fabiano. *Data protection and the fundamental right to guarantee the confidentiality and integrity of technical-informational systems in German law*. RJLB, Year, v. 5, p. 781-809, 2019.

**123.** Such rights define protected spaces, where intrusion by the State requires special justification. In this regard, this Supreme Court has rightly recognized that technological transformations demand a constant reassessment of how fundamental rights are affected and how the normative values of the Constitution can be made effective in light of new information technology mediations. Adequate protection of the free development of personality requires preventing the erosion of individual autonomy and reaffirming fundamental rights[75].

**124.** As was noted in the joint vote of ADI No. 6649 and ADPF No. 695, according to the Honorable Justice Gilmar Mendes:

> *In the digital age, new communication technologies have become a necessary condition for the realization of basic rights - as is evident in the field of freedom of expression, political and religious expression. (...) It is necessary that, faced with the threats generated by the development of technology, constitutional jurisdiction should act as an instrument of legal innovation, aiming to constantly update the protection of fundamental rights*[76].

**125.** The protection of privacy, broadly speaking, is essential for the proper exercise of various other fundamental rights. Additionally, the right to private life safeguards individuals from violations of the secrecy and freedom of their private life. This protection, in turn, prevents third-party interference by investigating events related to a person's personal and family life and their personal data. As is well known, the secrecy of private life is threatened by undue and unlimited investigations of electronic devices, exacerbated by the instruments currently under discussion, such as spyware.

**126.** **The protection of privacy must be even more rigorous in this case, as we are dealing with a powerful technological tool** that can infiltrate various aspects of an individual's life through constant and real-time monitoring.

**75** HOFFMANN-RIEM, Wolfgang. *General theory of digital law: challenges for the law*. Rio de Janeiro: Forense, 2020.

**76** BRAZILIAN SUPREME COURT. ADI No. 6649 & ADPF No. 695. Justice Gilmar Mendes' vote, p. 16-17.

**127.** In fact, José Afonso da Silva has previously expressed the risks of using technology to the detriment of the right to privacy:

> *The wide-ranging computerized information system leads to a process of scrutinizing people, who have their individuality completely taken from them. The threat is all the greater as the use of information technology facilitates the interconnection of files with the possibility of forming large databases that unveil people's lives without their authorization or even their knowledge*[77].

**128.** As widely discussed in legal doctrine, Danilo Doneda explains that the right to privacy is not to be confused with the autonomous right to personal data protection, which is associated with the principles of fair information practices and a set of procedures that enable the flow of personal data while reducing power asymmetries between data subjects and controllers. This is achieved through a series of risk mitigation strategies and institutional structures for enforcing data rights, such as the role played by Data Protection Authorities (DPAs)[78].

**129.** Therefore, based on a classic theoretical formulation by Stefano Rodotà, the protection of personal data is less related to "non-intrusion" and negative freedoms, and more related to the powers of control over personal data and positive freedoms in a democratic environment[79].

**130.** This theoretical formulation was well recognized by the Brazilian Supreme Court at the trial of ADI No. 6387 and ADI No. 6649. **The protection of personal data falls within the scope of personality rights and requires a set of positive obligations from the State for its effective enforcement**.

**131.** For this reason, this Court has correctly delineated a **subjective dimension** to personal data protection rights (the rights over data that can be exercised by citizens under the terms of the General Personal Data Protection Law) and

**77** SILVA. José Afonso da. *Positive Constitutional Law Course*. 34. ed. São Paulo: Malheiros, 2011, p. 209-2010.

**78** DONEDA, Danilo. *From Privacy to Personal Data Protection*. Second Edition. Rio de Janeiro: Revista dos Tribunais, 2001. P. 165

**79** DONEDA, Danilo. *From Privacy to Personal Data Protection*. Second Edition. Rio de Janeiro: Revista dos Tribunais, 2019. P. 39.

an **objective dimension** to these rights, which implies a set of safeguards and administrative procedures capable of reducing excessive risks to freedoms and the unfettered development of personality. Constitutional Amendment No. 115/2022 established the differentiation, pointing to data protection as an autonomous fundamental right in Article 5, item LXXIX.

132. **The Brazilian Supreme Court (STF) therefore recognizes that there are state duties to protect the values that structure the democratic regime, by creating institutional safeguards that preserve the essence of citizenship.**

133. In the present case, it is essential for the Court to comprehend how the surveillance tools operated by the State affect the system of individual guarantees systemically under the logic of informational self-determination.

134. Coined by the German Constitutional Court in the judgment on the Census Act (*Volkszählungsurteil*), informational self-determination limits the influence on individuals' behavior from the processing of personal data. It materializes personality rights and the dignity of the human person in light of new technologies, ensuring that individuals do not own their data, but rather have control over the information that third parties hold about them.

135. In the processing of data by public authorities, and especially given the tools for hacking into computer devices, **the informational asymmetry between the state and individuals accentuates the risks posed to the protection of personal data.** As the holder of a monopoly on coercive force, the powers of the public administration can in themselves lead to a series of violations of constitutional guarantees. The subject of this action further highlights this power relationship, insofar as the exploitation of technical vulnerabilities allows computer devices to be hacked without the knowledge of their targets.

## III.3. THE RIGHT TO THE INTEGRITY OF INFORMATIONAL SYSTEMS AS AN EXPRESSION OF THE CONSTITUTIONAL RIGHTS TO PRIVACY AND DATA PROTECTION

**136.** On several occasions, the Brazilian Supreme Court has had the opportunity to question the need for vigilance and investigative powers of the State, on the one hand, and the fundamental rights of citizens, on the other.

**137.** On these occasions, the Court has shown a strong tendency to **reinforce the State's responsibility not to weaken the security of its citizens' communications and thus to ensure a democratic infrastructure for public debate. Here are some examples of these cases.**

**138.** In the Action Against the Violation of a Constitutional Fundamental Right (ADPF) No. 722[80], for example, which discussed the unconstitutionality of a report drawn up by the Ministry of Justice and Public Security that identified a group of civil servants and teachers as members of the "anti-fascism movement" under the allegation of intelligence activity[81], Justice Cármen Lúcia emphasized that:

> ***the State's intelligence service**, for public security, national security and to guarantee the efficient fulfillment of the State's duties, is necessary, but **it cannot be conducted outside strict constitutional and legal limits, under penalty of compromising democracy in its most central instance, which is the guarantee of fundamental rights**. That is why it is certain that intelligence agencies at any hierarchical level of any of the powers of the state are also subject to the scrutiny of the judiciary[82].*

**80** BRAZIL. Brazilian Supreme Court. Action Against the Violation of a Constitutional Fundamental Right (ADPF) No. 772. Petitioner: *Rede Sustentabilidade*. Summoned: Minister of State for Justice and Public Security. Rapporteur: Justice Cármen Lúcia. Electronic Justice Gazette. Brasília, June 9, 2022. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5967354.

**81** TEIXEIRA, Lucas Borges. What it is, who made it and who is in the anti-fascist dossier. Uol explains, Aug. 18, 2020. Available at: https://noticias.uol.com.br/politica/ultimas-noticias/2020/08/18/uol-explica-oque-e-quem-fez-e-quem-atinge-o-dossie-antifascista.htm.

**82** BRAZIL. Brazilian Supreme Court. Action Against the Violation of a Constitutional Fundamental Right (ADPF) No. 772. Petitioner: *Rede Sustentabilidade*. Summoned: Minister of State for Justice and Public Security. Rapporteur: Justice Cármen Lúcia. Electronic Justice Gazette. Brasília, June 9, 2022. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5967354.

**139.** The Honorable Justice addressed the constitutional functions of intelligence agencies, excluding from the scope of the institution the preparation of dossiers that serve to profile and embarrass opponents, such as the anti-fascist dossier:

> ***Intelligence activities, therefore, must respect the democratic regime, which does not allow the persecution of opponents and the political apparatus of the State.*** *In fact, the history of reported abuses of the intelligence service emphasizes the need for effective control of this activity*[83].

**140.** And concluded that:

> *The collection of data, the production of information and the respective sharing between the bodies that make up the Brazilian Intelligence System must be strictly* ***linked to the public interest, democratic values and respect for fundamental rights and guarantees***[84].

**141.** In the Action Against the Violation of a Constitutional Fundamental Right (ADPF) No. 695[85], which questioned the constitutionality of government acts aimed at sharing data[86] contained in the DENATRAN database, which includes information on 76 million Brazilians, between bodies and entities that are not part of the Brazilian Intelligence System and Abin, Justice Gilmar Mendes argued that:

**83** *Ibidem*, p. 6.

**84** *Ibidem*, p. 8.

**85** BRAZIL. Brazilian Supreme Court. Action Against the Violation of a Constitutional Fundamental Right (ADPF) No. 695. Petitioner: Brazilian Socialist Party (PSB). Summoned: Federal Government. Rapporteur: Justice Gilmar Mendes. Electronic Justice Gazette. Brasília, 15 Sep. 2022. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693.

**86** Brazilian Supreme Court validates data sharing subject to requirements. STF, September 15, 2022. Available at: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=494227&ori=1.

> *The processing of personal data by the State is essential for the provision of public services. However, contrary to what the public entity asserts,* ***the discussion about privacy in relations with the State Administration should not start from a dichotomous view that places the public interest as a legal good to be protected in a totally different way and in confrontation with the constitutional value of privacy and protection of personal data***[87]*.*

**142.** As for the Direct Action for the Declaration of Unconstitutionality (ADI) No. 6529[88], the purpose of which was to interpret the sole paragraph of Article 4 of Law No. 9.883/1999 in such a way as **to require that the Brazilian Intelligence Agency's requests for information from bodies in the Brazilian Intelligence System be accompanied by reasons demonstrating the need for the data sought and the suitability of the request for the entity's legal purposes,** Reporting Justice Cármen Lúcia established the following thesis:

> *The nature of the intelligence activity, which may be conducted under a regime of secrecy or restricted publicity, does not remove the obligation to motivate administrative acts, especially considering that these acts may lead to access to sensitive data and information about citizens, limiting the fundamental rights to privacy and intimacy.*[89]

**143.** In ADIs No. 6.389, No. 6.390, No. 6.393, No. 6.388, and No. 6.387[90], in which the full court upheld a precautionary measure to suspend the effectiveness of Provisional Presidential Decree No. 954/2020. The Provisional Presidential Decree authorized

**87** BRAZIL. Brazilian Supreme Court. Action Against the Violation of a Constitutional Fundamental Right (ADPF) No. 695. Electronic Justice Gazette. Brasília, 15 Sep. 2022.

**88** BRAZIL. Brazilian Supreme Court. Action Against the Violation of a Constitutional Fundamental Right (ADPF) No. 6529. Petitioner: *Rede Sustentabilidade* and Brazilian Socialist Party (PSB). Summoned: Brazilian President and Brazilian Congress. Rapporteur: Justice Cármen Lúcia. Electronic Justice Gazette. Brasília, 22 Oct. 2021. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5972837.

**89** *Ibidem*, p. 25.

**90** BRAZIL. Brazilian Supreme Court. Action Against the Violation of a Constitutional Fundamental Right (ADPF) No. 6387. Petitioner: Council of the Brazilian Bar Association (CFOAB). Summoned: Brazilian President. Rapporteur: Justice Rosa Weber. Electronic Justice Gazette. Brasília, November 12, 2020. They were processed together by determination of the rapporteur, as both sought to challenge the constitutional validity of Provisional Presidential Decree No. 954/2020. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165.

the sharing of data belonging to millions of Brazilian fixed and mobile telephone users with the Brazilian Institute of Geography and Statistics (IBGE). In the action, Reporting Justice Rosa Weber **recognized the existence of an autonomous fundamental right to the protection of personal data and informational self-determination,** pointing out that:

> ***Such information, related to the identification - actual or potential - of a natural person, constitutes personal data and, to that extent, falls within the scope of protection of the constitutional clauses guaranteeing individual freedom (Article 5, head provision), privacy and the free development of personality (Article 5, items X and XII). Its manipulation and treatment must therefore comply with the limits set by constitutional protection, under penalty of damaging these rights.*** *As a result of personality rights, respect for privacy and informational self-determination have been enshrined in Article 2, items I and II of Law No. 13.709/2018 (General Personal Data Protection Law), as specific foundations for the discipline of personal data protection (ADI No. 6.387, p. 16 of the appellate decision).*

**144.** And concluded by explaining that:

> *(...) this cannot be done in a way that does not ensure protection mechanisms compatible with the constitutional clauses guaranteeing individual freedom (Article 5, head provision), privacy and the free development of personality (Article 5, X and XII). Just as requiring cars to be equipped with brakes, airbags and rear-view mirrors does not mean creating obstacles for the car industry, requiring rules involving fundamental and personality rights to meet minimum requirements of constitutional adequacy cannot be read as an impediment to state activity either. (ADI No. 6.387, p. 28 of the appellate decision).*

**145.** Therefore, over the years, **this Court has not only recognized the autonomous right to the protection of personal data and informational self-determination but has also conditioned the activities of the State to guarantee these rights and not to weaken the information and communication environment of its citizens.**

**146.** So far, this is also the prevailing interpretation in the cryptography debate.

**147.** In Brazil, arguments regarding the constitutionality of breaking encryption were first raised between 2015 and 2016, when the WhatsApp app was the target of four blockades by court orders throughout the country[91]. In these cases, the argument centered on the company's refusal to comply with judicial requests for access to its users' data. That same year, in order to discuss the controversial legal-constitutional issue at the heart of the blockades, there were at least two lawsuits before the Brazilian Supreme Court (ADPF No. 403[92] and No. ADI 5527[93]).

**148.** We would like to point out that the Justices of this Court have made extremely important contributions to the issue. **The ADPF and ADI trials are taking place together and the votes of the rapporteurs, Justice Edson Fachin and Justice Rosa Weber, respectively, bring lessons for the legal-constitutional treatment of the spyware issue.** These contributions are important because they offer interpretations of rights that are central to this case and do not reproduce reductionist simplifications of the problem. **We will briefly outline the background to the lawsuits on encryption, a summary of the arguments in the votes published so far and, finally, how these arguments can help to elucidate the present case.**

**91** G1. WhatsApp has already been blocked by court decision in 2015 and 2016 in Brazil. 18 Mar. 2022. Available at: https://g1.globo.com/tecnologia/noticia/2022/03/18/whatsapp-ja-foi-bloqueado-por-decisao-judicial-em-2015-e-2016-no-brasil.ghtml.

**92** BRAZIL. Brazilian Supreme Court. Action Against the Violation of a Constitutional Fundamental Right (ADPF) No. 403. Petitioner: Citizenry. Summoned: Judge of the Criminal Court of the District of Lagarto. Rapporteur: Justice Edson Fachin. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500.

**93** BRAZIL. Brazilian Supreme Court. Action Against the Violation of a Constitutional Fundamental Right (ADPF) No. 5.527. Petitioner: Republican Party. Summoned: Brazilian President and Brazilian Congress. Rapporteur: Justice Rosa Weber. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282.

**149.** In short, both actions refer to the extension of Article 12 of the Brazilian Civil Rights Framework for the Internet, albeit in different ways[94]. However, **the mediate controversial legal issue, and the one that interests us for this contribution, is the interpretation of the constitutional right to privacy and due process of law and, thus, the guarantees owed to citizens in the context of investigations into digital communications in Brazil.** Next, we will briefly review the contributions from the votes of Justices Rosa Weber and Edson Fachin, in ADI No. 5527 and ADPF No. 403, respectively. Here, the focus will be especially on the arguments the justices made about the State's responsibilities in relation to telecommunications infrastructure and informational systems.

**150.** In her vote[95] in ADI No. 5527, the rapporteur and former Justice of this Court, Rosa Weber, recognizes the virtualization of individuals' privacy and equates mobile devices, for example, with "*luminous windows into our intimacy*"[96]. Weber argues that cell phones "*keep much more of the private life and intimacy of their owners than the doors and walls, drawers and cupboards of each one's home, **and that we have no difficulty in recognizing the inviolability of the home.***"[97]

**151.** Given the legislative framework and precedents for safeguarding rights, the Justice rightly decides that the **State does not have the power to force companies that "*provide private communications services to adopt mechanisms that ensure access to the content of conversations*"[98] and thus weaken their encryption.** Weber goes further and argues that encryption has played a central role in the

**94** It is debated whether Article 12 pertains solely to the violation of rules regarding the protection of records, personal data, and private communications as set forth in Articles 10 and 11, or whether its interpretation also extends to the non-compliance with judicial orders requesting access to personal data for the purpose of criminal prosecution. ADPF No. 403 challenges one of the decisions that blocked WhatsApp and asks the Brazilian Supreme Court to prohibit judicial orders aimed at suspending private messaging services, such as WhatsApp, on the grounds that such acts violate the 'right to communication' of thousands of citizens. On the other hand, ADI No. 5527 seeks the unconstitutionality of Article 12, III and IV of the Brazilian Internet Civil Framework (Marco Civil da Internet), which provides for sanctions of suspension and prohibition of activities for internet platforms and services, and requests that only decisions made in the context of criminal prosecution may allow the breach of confidentiality of communications on these platforms.

**95** BRAZIL. Brazilian Supreme Court. Direct Action for the Declaration of Unconstitutionality (ADI) No. 5.527. Vote by Justice Rosa Weber. 36 pages. Available at: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf.

**96** BRAZIL. Brazilian Supreme Court. Direct Action for the Declaration of Unconstitutionality (ADI) No. 5.527. Vote by Justice Rosa Weber. 36 pages. Available at: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf, p. 6.

**97** *Ibidem*, p. 7.

**98** *Ibidem*, p. 27.

effective protection of human rights such as freedom of expression and privacy, but also **security** itself. According to Justice Weber:

> *The trade-off here, therefore, is not between public security and privacy, because* ***a claim that threatens privacy****, even if it is based on countering an immediate security threat, also* ***violates the security of networks and their users as a whole in the long term****, exposing them to greater risks of cyber-attacks, fraud, identity theft, invasion of privacy, extortion, etc*[99]*.*

**152.** In **ADPF No. 403**[100], Reporting Justice Edson Fachin agreed, for the most part, with the arguments and conclusions of Justice Rosa Weber. It should also be noted that both actions had contributions from the same public hearing[101].

**153.** The Honorable Justice Fachin provides a summary of his vote based on the seven basic premises of the argument. The first five premises reaffirm the arguments that: i) technological advances must be accompanied by an updating of the scope and guarantee of fundamental rights; ii) rights extend to the digital world; iii) the right to privacy and freedom of expression are conditions for the full exercise of access to the internet; iv) privacy is the right to maintain control over your information and to determine how to construct your own public sphere; v) freedom of expression is an essential condition for the pluralism of ideas, a structural vector of the democratic system of law[102].

**154.** The sixth and seventh premises **relate directly to the centrality of protecting the security and integrity of communications systems in order to protect fundamental rights such as privacy and freedom of expression.**

**99** *Ibidem*, p. 31.

**100** BRAZIL. Brazilian Supreme Court. Action Against the Violation of a Constitutional Fundamental Right (ADPF) No. 493. Justice Edson Fachin's vote. 76 pages. Available at: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf.

**101** InternetLab. Open Court Hearing on WhatsApp Encryption and Blocking: arguments before the Brazilian Supreme Court. ABREU, Jacqueline. 29 jun. 2017, Available at: https://internetlab.org.br/pt/noticias/audienciapublica-sobre-criptografia-e-bloqueios-whatsapp-argumentos-diante-stf/.

**102** BRAZIL. Brazilian Supreme Court. Action Against the Violation of a Constitutional Fundamental Right (ADPF) No. 493. Justice Edson Fachin's vote. 76 pages. Available at: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf, p. 1-2.

**155.** The Justice **points out that encryption, as well as anonymity, guarantee the development and sharing of opinions** and are closely related to freedom of expression. He also argues that it is contradictory that *"in the name of public security, we should stop promoting and seeking a safer internet. A safer internet is everyone's right and the State's duty."*[103] **In his last premise, Justice Fachin dispels the false dilemma between security and privacy, and argues that weakening encryption also offends the State's duty to provide security**. Thus, the Justice decides to uphold the ADPF to:

> *declare the partial unconstitutionality without reduction of text of both item II of Article 7 and item III of Article 12 of Law No. 12.965/2014,* ***in order to rule out any interpretation*** *of the provision* ***that authorizes a court order requiring exceptional access*** *to the content of an end-to-end encrypted message* ***or that, by any other means, weakens the cryptographic protection of internet applications.***[104]

**156.** Both votes allow us to argue that we have a right to integrity and security when using computer and communication systems.

**157.** Personal data protection is a prerequisite for the engagement of individuals in public issues and a functional prerequisite for democratic communication. According to constitutional law doctrine, the rules on the protection of personal data and the integrity of computer systems create the conditions for the continuity of the democratic rule of law. As recognized by Professor Fabiano Menke, *"the fundamental right to guarantee the confidentiality and integrity of technical-informational systems updates the protection of personality to the technological reality of the 21st century"*[105]. This right is linked to constitutional norms protecting the dignity of the human person and freedom. The recognition of this right operates as a normative barrier, considering that its restriction can only occur when there are clear postulates of proportionality, adequacy, and necessity.

**103** *Ibidem*, p. 2.

**104** BRAZIL. Brazilian Supreme Court. Action Against the Violation of a Constitutional Fundamental Right (ADPF) No. 493. Justice Edson Fachin's vote. 76 pages. Available at: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf, p. 73.

**105** MENKE, Fabiano. Data protection and the fundamental right to guarantee the confidentiality and integrity of technical-informational systems in German law. *RJLB*, Year, v. 5, 2019, p. 801-802.

158. **It is therefore concluded that the State is not only prohibited from making these systems vulnerable, but also has a duty to protect and improve them. For this very reason, the use of remote intrusion technologies should be considered unconstitutional, given the damage it causes to the security and integrity of communication systems and users' rights.**

## IV. ON THE ANALYSIS OF NECESSITY AND PROPORTIONALITY IN THE USE OF SPYWARE IN CRIMINAL INVESTIGATIONS

159. Once the existence of an autonomous right to the integrity of informational systems, which compels the State to refrain from acquiring remote intrusion technologies, has been defended, we then move on to consider the use of such tools in light of constitutional and nonconstitutional norms, as well as the guarantees of criminal procedural law.

160. **We argue in this section that there is no balance between necessity and proportionality in the use of remote intrusion tools. Even if the required checks and balances are considered, the legal safeguards that currently exist in relation to data breach and interception are not sufficient to support the use of these tools.**

### IV.1. DATA CONFIDENTIALITY BREACH: FOUNDATIONS AND LIMITS

161. Breaches in confidentiality are certainly possible under Brazilian law, but it must adhere to explicitly established legal boundaries. Our legal system outlines different and specific procedures for public authorities to access personal data in the context of criminal investigations. These are significant legal restrictions aimed at giving effect to constitutionally protected fundamental rights.

162. In this respect, the Telephone Interception Law (Law No. 9.296/1996) allows the "interception of the flow of communications in computer and telematic systems" in certain cases but prohibits it if there are no "*reasonable indications of authorship or participation in a criminal offense*" (Article 2, I).

**163.** Similarly, the Code of Criminal Procedure (CPP) provides for the possibility of obtaining location data relating to an ongoing crime of human trafficking[106], so that the victim and suspects can be located, and, in the case of the Telephone Interception Law, the possibility of accessing these communications in certain cases, provided that reasonable evidence of the authorship of the crime being investigated can be demonstrated.

**164.** Furthermore, the Money Laundering Law (Law No. 9.613/1998, amended by Law No. 12.683/2012) and the Criminal Organization Law (Law No. 12.850/2013) provide for the need for specific judicial authorization to obtain data on the investigated person that goes beyond their personal qualifications, affiliation, and address. Once again, different legislation has been added to the established interpretation of the constitutional text restricting the intrusions into citizens' lives.

**165.** According to the provisions of Article 17-B of Law No. 9.613/1998 and Article 15 of Law No. 12.850/2013, regardless of judicial authorization, to "*the investigated person's registration data that exclusively informs the personal qualification, affiliation and address held by the Electoral Justice, telephone companies, financial institutions, internet providers and credit card administrators*". **Conversely, any other types of data will only be obtained with a specific court order, which addresses and explains the need for that extreme measure to breach data confidentiality.**

**166.** Furthermore, the Brazilian Civil Rights Framework for the Internet, recognizing the protection of privacy and data secrecy as general principles of the Internet and as users' rights (Articles 3, 7 and 8), allows the provision of connection records (Article 5, VI) and access to applications (Article 5, VIII) of users involved in unlawful acts committed on the Internet, but expressly requires a court order based on well-founded evidence of unlawful acts and a reasoned justification for the usefulness of the data requested (Article 22).

**106** "Article13-B. If necessary for the prevention and repression of crimes related to human trafficking, the member of the Public Prosecutor's Office or the police chief may request, by means of judicial authorization, that companies providing telecommunications and/or telematics services immediately make available the appropriate technical means - such as signals, information and others - that allow the victim or suspects of the crime in progress to be located."

**167.** In other words, under exceptional circumstances in which the public interest overrides the private interest in the inviolability of communications or data secrecy, which are inherent to the constitutionally protected right to privacy, it is necessary to obtain a specific, reasoned, and individualized court order. This is an unavoidable condition for conducting the exceptional measure of breaching the confidentiality of such constitutionally protected data.

**168.** There is no possibility of remote intrusion into electronic devices in any of the cases covered by Brazilian law. On the contrary: Brazilian law establishes a necessary relationship between the use of personal data in investigations, on the one hand, and elements that demonstrate the potential involvement of the affected individual in illegal activities, on the other.

## IV.2. ON THE ABSENCE OF NECESSITY AND PROPORTIONALITY IN THE USE OF SPYWARE TOOLS IN CRIMINAL INVESTIGATIONS

**169.** Based on the topic above, we conclude that **any interception, request, sharing, or breach of data confidentiality must be clearly justified. This justification should align strictly with the law** and be the result of a careful balancing between the public interest in criminal investigations and the significant risks posed to the fundamental rights and freedoms of the data subject.

**170.** In this regard, it is important to highlight Brazil's adherence to the International Covenant on Civil and Political Rights (ICCPR) and the American Convention on Human Rights (Pact of San José, Costa Rica), which protect everyone's rights to opinion and freedom of expression, ensuring protection against arbitrary and abusive interference in private life. This protection extends to private communications and the data associated with such communications.

**171.** Any restrictions on these rights, according to Article 19 of the Covenant and as defined by the Inter-American Court of Human Rights[107], must comply with a tripartite test that requires, at a minimum, adherence to the following

**107** The application of the tripartite test for verifying the legitimacy of interferences in privacy in the field of communications was affirmed by the Inter-American Court of Human Rights (IACHR) in the cases of Tristán Donoso v. Panama and Escher et al. v. Brazil.

criteria: **(a) they must be legally defined and limited, (b) they must meet the criteria of necessity and proportionality, and (c) they must be necessary to achieve a legitimate objective**, such as national security, public order, public health, or morals.

**172.** Thus, the State bears the burden of proving a direct and immediate connection between a potential threat and the consequent restriction of rights, as well as of imposing the least intrusive measure among those capable of achieving the same protective function.

**173.** As highlighted by Justice Carmen Lúcia in her vote in the Direct Actions for the Declaration of Unconstitutionality Nos. 6.387, 6.388, 6.389, 6.390, 6.393[108]:

> *In cases of restrictions on the right to privacy, International Human Rights Law requires that the limit be legally defined and only legitimizes it if it is to achieve a legitimate objective (...) and provided that it is deemed necessary and proportional to the objective sought[109].*

**174.** When detailing the requirements of necessity and proportionality in Advisory Opinion OC-5/85[110], the Inter-American Court of Human Rights emphasized that it **is not enough to demonstrate that the restriction serves a useful or opportune purpose, but it must be justified according to a legitimate objective that clearly prevails over the social need for the full enjoyment of the right and does not limit the protected right more than is strictly necessary.**

**108** They were processed together by order of the rapporteur, Justice Rosa Weber, as both sought to challenge the constitutional validity of the Provisional Presidential Decree No. 954/2020.

**109** BRAZIL. Full Brazilian Supreme Court. Direct Action for the Declaration of Unconstitutionality (ADI) No. 6.387. PROVISIONAL MEASURE IN DIRECT ACTION FOR THE DECLARATION OF UNCONSTITUTIONALITY. REFERENDUM. PROVISIONAL PRESIDENTIAL DECREE NO. 954/2020. PUBLIC HEALTH EMERGENCY OF INTERNATIONAL IMPORTANCE DUE TO THE NEW CORONAVIRUS (COVID-19). THE SHARING OF USER DATA FOR THE FIXED SWITCHED TELEPHONE SERVICE AND THE PERSONAL MOBILE SERVICE BY THE PROVIDERS WITH THE BRAZILIAN INSTITUTE OF GEOGRAPHY AND STATISTICS. FUMUS BONI JURIS. PERICULUM IN MORA. GRANT REQUESTED. Rapporteur: Justice Rosa Weber, May 07, 2020. Lex. Available at: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629.

**110** INTER-AMERICAN COURT OF HUMAN RIGHTS. Advisory Opinion OC-5/85. The compulsory registration of journalists (Articles 13 and 29 of the American Convention on Human Rights). 13 Nov. 1985. Available at: https://www.corteidh.or.cr/docs/opiniones/seriea_05_por.doc

**175.** With regard to access to data associated with communications, the Special Rapporteurs for Freedom of Expression of the United Nations and the Inter-American Commission on Human Rights (IACHR) have repeatedly stressed that mass surveillance does not meet the proportionality requirement, even if it serves a legitimate purpose (UN, A/HRC/27/37)[111]; IACHR/RELE/INF.17/17)[112].

**176.** This raises the question of when and if the use of state-directed surveillance tools could be considered proportional under the scrutiny of humanitarian law. In other words: considering that the existence of a law and a court order would be minimum parameters for the possibility of using these tools, **would it be possible to think of legitimate objectives that would justify considering these measures as necessary and proportionate in exceptional cases?**

**177.** **Spyware tools are among the most intrusive instruments available to the Government.** The possibility of remote access to an electronic device without the user's knowledge should not be equated with telephone interception or home invasion since the degree of intrusiveness of the measure on private life can be considered even worse[113]. Information from an electronic device can reveal profound aspects of its owner's digital identity, from their home to their habits, income, people they meet, etc. As such, it forms a comprehensive and private portrait of an individual's private life: their lifestyle habits, interests, preferences, family, political, professional, religious, and sexual associations can be revealed or inferred.

**111** REPORT OF OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS. *The right to privacy in the digital age. UN Doc. A/HRC/27/37*, June 30, 2014. Translation. Instituto de Referência em Internet e Sociedade. p. 12. Available at: https://irisbh.com.br/wpcontent/uploads/2022/12/O-direito-a-privacidade-na-era-digital-Relatorio-do-Gabinete-do-AltoComissariado-das-Nacoes-Unidas-para-os-Direitos-Humanos.pdf.

**112** ORGANIZATION OF AMERICAN STATES SPECIAL RAPPORTEUR ON FREEDOM OF EXPRESSION. Writ of execution of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur on freedom of expression of the Inter-American Commission on Human Rights. OAS IACHR/RELE/Art. 41/7-2020/65. July 3, 2020. Available at: https://www.oas.org/es/cidh/expresion/documentos_basicos/PORTCARTAONUCIDHBRASILINTERNET2020.pdf.

**113** ANTONIALLI, Dennys. ABREU, Jacqueline. *And when the policeman becomes a hacker?* INTERNETLAB, Jul. 17, 2017, Available at: https://internetlab.org.br/pt/noticias/e-quando-o-policial-vira-hacker/.

**178.** Notwithstanding the extent of the power of surveillance in these cases, intrusions of this kind can allow the investigating officer to use the device as if he were the investigated person, **which can severely compromise the reliability of the evidence that results from this means[114] and therefore creates challenges for the preservation of the chain of custody.**

**179.** There are currently countless other investigative techniques and tools available to the State, which are less damaging than directly hacking into an electronic device. Given the advance of information and communication technologies and the profusion of means of obtaining digital evidence, it is possible to identify the perpetrators of crimes through ordinary means of investigation, especially through procedures that are less restrictive of rights.

**180.** Therefore, there would seem to be no exceptional cases justifying the implementation of such an intrusive measure as a spyware tool. **It is therefore unreasonable to assume that the use of spyware would be "necessary and proportionate" in any case.**

**181.** Even if it is considered that a balance between risks and benefits should be made on a case-by-case basis, the fact is that our current regulatory framework is not sufficiently adequate to support the use of such tools without them seriously jeopardizing the democratic environment and the civil rights and freedoms of all Brazilian citizens.

**182.** It is therefore concluded that the use of spyware-type tools by the State is unconstitutional. In fact, it has been shown that these tools have the corollary of buying and selling vulnerabilities in the information security of all citizens of democratic societies. As a result, the fundamental rights of privacy, security of communications and image, among others, are violated. Thus, it is not possible for the State to acquire any type of remote intrusion technology, as there is a serious threat to the Democratic Rule of Law. On the other hand, the right to the integrity of informational systems must be defended, an idea that is in line with constitutional guarantees.

**114** ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (coord.). *The right to digital investigations in Brazil: foundations and regulatory frameworks*. São Paulo: InternetLab, 2022. p.73. Available at: https://internetlab.org.br/wp-content/uploads/2022/10/INTERNETLAB_O-DIREITO-DAS-INVESTIGACOES_PRINT_10-2022.pdf

# V. ON THE RESIDUAL HYPOTHESIS OF THIS HONORABLE COURT DECIDING ON THE NECESSITY OF USING SPYWARE TOOLS

**183.** Alternatively, in the event that this Honorable Supreme Court does not find the use of spyware by the State unconstitutional, despite the extensive arguments presented above, it is imperative to establish a specific framework to address the indiscriminate use of these technologies, in order to provide adequate and effective protection to the fundamental rights impacted by such mechanisms.

**184.** This constitutional framework for the use of remote virtual intrusion tools must, at a minimum, consider the following: (i) the necessity of prior judicial authorization and adherence to the same rigor applied to other situations involving breaches of confidentiality; (ii) a constitutional interpretation of the right to privacy in communications that is updated to reflect contemporary levels of intrusiveness; (iii) the inclusion of mechanisms that ensure respect for the chain of custody; (iv) the individualization of subjects targeted by intrusion procedures; (v) the development of additional parameters compatible with the constitutional order. These elements should be explicitly included in any injunction directed to the Brazilian Congress, as they directly stem from a proper constitutional interpretation of the situations addressed in this case.

## V.1. ON THE NECESSITY OF PRIOR JUDICIAL AUTHORIZATION AND THE APPLICATION OF EQUAL RIGOR AS IN OTHER SITUATIONS INVOLVING BREACHES OF CONFIDENTIALITY, ALONG WITH OTHER PARAMETERS IN ACCORDANCE WITH THE EXISTING LEGAL FRAMEWORK

**185.** Certainly, in a Democratic State of Law, as is the case in Brazil, the use of remote virtual intrusion tools cannot be conceived of without a **prior judicial decision** demonstrating the need, appropriateness, and proportionality of the measure, in order to safeguard the guarantees of intimacy, privacy and confidentiality of data and communications. On the contrary, the level of protection of fundamental rights will be unjustifiably and arbitrarily reduced.

**186.** Indeed, considering the impact it has on the lives of individuals and the effects on the exercise of fundamental rights and freedoms in a Democratic State of Law, it is indisputable that the use of spyware must comply with certain criteria: i)

subjection to specific law; ii) compliance with strict requirements, in a treatment analogous to the existing regulations for other hypotheses of confidentiality breach; iii) stipulation of a reasonable period of duration (with provision for extension or not); iv) individualization of the targets of the measure; v) exclusive targeting for criminal investigation and criminal procedural instruction; vi) preservation of the chain of custody, among other specifications.

**187.** In this respect, it is possible to glimpse, in current national legislation, a regulatory framework that can be used as a basis for establishing its own regulations on the use of remote virtual intrusion programs and secret and invasive monitoring tools, aimed at establishing the requirements and formalities necessary for this type of activity.

**188.** In regulating the interception of telephone communications, Law No. 9.296/1996, for example, determines that the measure depends on reasoned judicial authorization, as well as establishing minimum requirements that can also guide the standards to be established regarding the matter in question. For example:

> *Article 2. Interception of telephone communications will not be allowed when any of the following occur:*
> *I – there is no reasonable evidence of authorship or participation in a criminal offense;*
> *II – the evidence can be provided by other available means;*
> *III – the fact under investigation constitutes a criminal offense punishable, at most, by imprisonment.*
> *Sole paragraph. In any event, the situation under investigation must be clearly described, including the names and qualifications of those being investigated, unless this is clearly impossible and duly justified.*
>
> *Article 3. The interception of telephone communications may be ordered by the judge, either ex officio or at request from:*
> *I – the police authority, in criminal investigations;*
> *II – the Public Prosecutor Office, in criminal investigations and in criminal proceedings.*

**189.** It also stipulates that the measure may not exceed a period of fifteen days, and that in order to renew it - for an equal period of time - evidence of the indispensability of the means of proof is required (Article 5).

**190.** Moreover, Law No. 13.964/2019 provides for the environmental capture of electromagnetic, optical, or acoustic signals, with subsidiary application of the rules on telephone and telematic interception. According to the specific regulation, the application for the measure must contain a detailed description of the location and method of installation of the environmental capture device. Furthermore, it should be demonstrated that the evidence or information to be obtained cannot be obtained by other means of proof, and the collection may not last more than fifteen days, renewable by means of a new reasoned court decision.

> *Article 8-A. For criminal investigation or instruction, the environmental capture of electromagnetic, optical, or acoustic signals may be authorized by the judge, at the request of the police authority or the Public Prosecutor's Office, when: (Included by Law No. 13.964/2019)*
> *I – the evidence cannot be provided by other available and equally effective means; and (Included by Law No. 13.964/2019)*
> *II – there is reasonable evidence of authorship and participation in criminal offenses with maximum sentences of more than four (4) years or related criminal offenses. (Included by Law No. 13.964/2019)*
> *§ 1º The application must describe in detail the location and method of installation of the environmental capture device. (Included by Law No. 13.964/2019)*
> *§ 2º The installation of the environmental capture device may be carried out, when necessary, by means of an undercover police operation or at night, except in the home, under the terms of item XI of the head provision of Article 5 of the Brazilian Constitution. (Included by Law No. 13.964/2019 (In force)*
> *§ 3º . Environmental capture may not exceed a period of 15 (fifteen) days, renewable by court decision for equal periods, if the indispensability of the means of proof is proven and when permanent, habitual, or continuous criminal activity is present. (Included by Law No. 13.964/2019)*

> *§ 4º The environmental capture made by one of the parties without the prior knowledge of the police authority or the Public Prosecutor's Office may be used in defense matters when the integrity of the recording is demonstrated. (Included by Law No. 13.964/2019) (In force)*
> *§ 5º The rules laid down in the specific legislation for telephone and telematic interception apply subsidiarily to environmental capture. (Included by Law No. 13.964/2019)*

**191.** Another issue of great relevance is the disposal of evidence, especially when, by means of the provisional measure, information is obtained from third parties, or even from the investigated parties themselves, but which involves data that is irrelevant to the purpose of the investigative and supervisory activity, and which may compromise the private sphere of the individuals in question, given their sensitivity. In these situations, the information obtained should only be partially preserved, discarding everything that is not useful or necessary, always under the supervision of the controlling authorities. This is what Article 9 of the aforementioned federal legislation stipulates:

> *Article 9. Any recording that is not relevant to the evidence shall be rendered inadmissible by a judicial decision, during the investigation, the trial proceedings, or thereafter, upon request by the Public Prosecutor or the interested party.*
> *Sole Paragraph. The incident of inadmissibility shall be assisted by the Public Prosecutor, and the presence of the accused or their legal representative shall be optional.*

**192.** It is also important to note the provision contained in Article 8 of Law No. 9.296/1996, which mandates the need to **preserve confidentiality** of the investigations, recordings, and transcriptions conducted under its authority.

**193.** In this normative microsystem aimed at the protection of data and communications, it is also possible to extract important boundaries established by Law No. 12.965/2014 (Brazilian Civil Rights Framework for the Internet), such as minimum requirements for **judicial requests** to lift the confidentiality of connection records or access to internet applications. According to Article 22 of the legislation, the investigating authority, in order to request access to telematics data with the aim of gathering evidence in criminal proceedings, must demonstrate well-founded

indications of the occurrence of a crime, providing a reasoned justification for the requested records, as well as specifying the respective period to which they refer.

194. Furthermore, despite the inapplicability of Law No. 13.709/2018 (General Data Protection Law) to the activities of investigation and prosecution of criminal offenses (Article 4, III, d), its principled basis is of essential relevance to ensure constitutional guarantees related to the processing of personal data, insofar as it provides for compliance with the principles of purpose, adequacy, necessity, security, prevention, among others (Article 6).

195. Ultimately, what we are attempting to reveal is that the absence of a proper regulatory framework to protect the use of spyware, with the imposition of limits, requirements, procedures, and legal processes, undermines legal certainty and the efficient protection of fundamental rights related to intimacy and privacy, giving room for abuses by investigation bodies and authorities, to the detriment of constitutionally guaranteed rights.

## V.2. CONSTITUTIONAL INTERPRETATION OF THE CONFIDENTIALITY OF COMMUNICATIONS UPDATED TO CONTEMPORARY STANDARDS OF INTRUSIVENESS

196. The fact is that **merely requiring a court order in cases of remote virtual intrusion is an insufficient measure to guarantee equal constitutional rigidity to other confidentiality-breaking mechanisms** - especially since constitutional interpretation must be based on the parameter of greater protection precisely in cases where there is greater potential for damage to a fundamental right.

197. In practical terms, remote intrusion into data stored on an electronic device, for example, involves a much more significant breach of information about a citizen's life than capturing a snippet of a telephone conversation. We're talking about all the conversations that may have taken place on a messaging app, all the emails exchanged, the subject's location and many other details.

198. Thus, the legislation that regulates the conditions for breaching confidentiality must be interpreted taking into account the contemporary conditions of the

technological evolution of communications. By doing so, this Court will give full effect to the constitutional mandates to protect privacy and intimacy (Article 5, X of the Brazilian Federal Constitution) and confidentiality (Article 5, XII of the Brazilian Federal Constitution), in light of rapid technological development.

**199.** To this end, it is important to immediately point out the inadequacy of the 'in flow – static' dichotomy to adequately describe data transmission on the internet and, consequently, to serve as a criterion for (un)protection. Therefore, the protection established in item XII of Article 5 of the Brazilian Federal Constitution should be applied, from which the greater protection provided, for example, by the aforementioned Law No. 9.296/1996, is derived.

**200.** Drawing parallels with telephone and telegraph communications has not proved adequate to address the risks associated with data communications, which can be understood as the transfer of signals, written messages, images, sounds, data, or intelligence - not necessarily components of a communicative process between subjects - through an electronic system.

**201.** Unlike a letter, the delivery of which delimits the end of the transmission, and the storage of which takes on a spatial dimension, the end of data transmission is often arbitrary and, in terms of its content, also reversible, given the possibility of subsequent editing. The storage of data by a device (remote or not) is, in this sense, far removed from the notion of static conservation. This argument is the result of the updating of an entire field of study that is showing clear signs of development, and it is true that one of the defenders of this position of less protection for "static" data before this Court, Professor Tercio Sampaio Ferraz Júnior, recently revised his position at a Congress organized by InternetLab. Here is a particularly enlightening excerpt:

> *"It's important to note, in this regard, that the confluence of technology - a case in point being the cell phone - has altered the traditional perception of the relationship between flow and stored data. Just look at how easy it is to copy and paste in the flow of communication. In order to understand this, there must inevitably be a balance between the individual's right to free communication (freedom of and right to information) and the value attributable to the promotion of public security (inviolability of confidentiality). This*

*particularly affects the hypothesis of a judicial authorization for any privileged access on the part of a state agent (criminal investigation), which must then take into account the possibility of a vulnerability to the communication system in the context of the inviolability of communication in terms of a private/social content, nuclear individuals in an access system. This means that the guarantee of a fundamental right to the confidentiality and integrity of systems implies to users that the disruption of anyone's privacy, when there is no probable cause, is incompatible with the model enshrined in the Brazilian Federal Constitution, since the breach of confidentiality cannot be arbitrarily manipulated by the government.* ***If this were not the case, confidentiality breaches would illegitimately become an instrument of generalized search, which would give the government - despite a court order - the power to rummage through the confidential records of indeterminate people, without any concrete evidence, in order to make it possible, through an illegal use of the indiscriminate search procedure (which not even the Executive Power can order)****, to access data supposedly impregnated with legal-probative relevance, depending on the information that might be discovered.*[115]"

**202.** Therefore, **a contemporary reading and comprehension of Article 5, XII, of the Brazilian Federal Constitution is urgently called for**, as even those who argued that its interpretation from decades ago should be guided by the 'static - in flow' dichotomy now understand that it does not capture the peculiarities of data communication and gives rise to abuses, fortunately circumvented by Brazilian courts.

**203.** This is the case of appeal in Habeas Corpus No. 99.735/SC, ruled on November 27, 2018, by the Superior Court of Justice, against a court order that authorized, based on the Telephone Interception Law, access to communications, through the

**115** FERRAZ JR, Tercio Sampaio Ferraz. "Data Privacy, the Right to Privacy, and the Limits of State Power: 25 Years Later." In: ANTONIALLI, D.; ABREU, J. (eds). *Fundamental Rights and Criminal Procedure in the Digital Age: Doctrine and Practice in Debate.* Vol. 1. InternetLab: São Paulo, 2018, pp. 103-104.

seizure of the mobile device and subsequent "mirroring", in the WhatsApp Web modality. In this case, an analogy between the institute of telephone interception (Article 1 of Law No. 9.296/1996) and the measure of mirroring was recognized by the unlimited access to past, present, and future conversations, with automatic updating, and the possibility of editing, which makes it impossible to control any information that may be brought to the case file.

**204.** Most consistent with the technical aspects of data communication and the risks experienced in the digital age is the position indicated in Justice Rosa Weber's vote in ADI 5527, according to which the availability of the content of private communications - whether in flow or stored - can only be determined by a "*judicial court order, in the cases and in the manner established by law", operating within the "semantic field demarcated by Article 5, XII, of the Brazilian Federal Constitution, (...) for the purposes of criminal investigation or criminal procedural instruction".* Storage, therefore, does not rule out the need for protection.

**205.** Thus, a contemporary reading of Article 5, XII of the Brazilian Federal Constitution on the issues in question is essential. Even those who once defended an interpretation based on the binomial "stored - streaming" now understand that such a view does not cover the peculiarities of data communication, allowing for possible abuses. **Therefore, a disproportionate protection of streaming data is outdated and counterintuitive for current times and will not offer the degree of protection that the most contemporary and appropriate constitutional interpretation of communications confidentiality requires.**

## V.3. INCLUSION OF MECHANISMS TO ENSURE RESPECT FOR THE CHAIN OF CUSTODY

**206.** In addition to the need for a prior judicial decision, the observance of parameters that already exist in the legal system, such as the provision of a maximum time limit for the measure, the discarding of evidence that is not related to the subject under investigation, etc. and the protection of data in flux, the **guarantees relating to the chain of custody must be observed.**

**207.** Observing the chain of custody ensures that the **integrity and authenticity of evidence collected during an investigation is maintained.** This is a fundamental

measure for securing the reliability of evidence and preserving its validity in criminal prosecution, as well as protecting individual rights and avoiding the collection of illegal evidence.

**208.** The particularities of digital evidence require legislative intervention to establish specific rules for the chain of custody, considering the production, admission, and valuation phases. Specific techniques must therefore be included for the individualization and seizure of this evidence, otherwise it will be rendered useless[116].

**209** Digital evidence is characterized by **dematerialization** and **dispersion.** In other words, digital evidence is volatile and fragile[117], which requires greater concern over forgery or destruction - it can be easily altered, which by its very nature allows for contamination, so it must be handled with greater care.

**210.** It is therefore necessary to develop techniques for constructing usable evidence when dealing with evidence obtained through digital means, such as spyware. Among other things, after obtaining the digital data, the data must be stored in a secure and appropriate location, with an analysis of the data obtained that is relevant to the subject of the investigation. Additionally, it is essential to present the evidence in court along with the production of expert evidence and any clarifications from experts.

**211.** Documenting the chain of custody is crucial, especially when analyzing digital data, in order to rule out possible improper alterations to the material obtained. Therefore, it is necessary to attach a technical report with an extensive description of the computer systems used, the instruments and the data obtained.

**116** BADARÓ, Gustavo. The chain of custody of digital evidence. Article prepared for the presentation of a lecture, with the same theme, at the International Congress on Probative Law, held on November 18 and 19, 2021, in Porto Alegre/RS, by the Pontifical Catholic University of Rio Grande do Sul and Alberto Hurtado University, with the support of IBDP and Procnet. Available at: https://edisciplinas.usp.br/pluginfile.php/8351444/mod_resource/content/0/BADARO%CC%81%20%20A%20cadeia%20de%20custo%CC%81dia%20da%20prova%20digital%20PUCRS.pdf

**117** Characteristics of digital evidence are non-materiality, volatility and fragility, which demand greater concern, cf. MASSENA, Caio Badaró. Regarding the chain of custody of digital evidence in criminal proceedings: brief notes on the logic of mistrust, informational asymmetry and the right to a defense, Boletim IBCCRIM, n. 368, Jul. 2023, p. 19-21.

**212.** It is recalled that the chain of custody was regulated between Articles 158-A and 158-F of the Code of Criminal Procedure, following Law No. 13.964/2019. Therefore, the documentation of the chain of custody was established as: "*The chain of custody is considered to be the set of all procedures used to maintain and document the chronological history of the evidence collected at crime scenes or from victims, in order to track its possession and handling from its recognition to its disposal,*" as established by Article 158-A.

**213.** This refers to the succession of all those who have had contact with the source of evidence, from the moment it is collected until it is presented in court. This means that all persons who have had contact with the evidence, as well as all the specific moments when they have had contact, must be documented, and all those involved in the chain of custody are responsible for recording and properly handling it (Article 158-D, §4, CPP).

**214.** Furthermore, the stages of the chain of custody were outlined in Article 158-B of the Code of Criminal Procedure, which are: (i) recognition; (ii) isolation; (iii) documentation; (iv) collection; (v) securing; (vi) transportation; (vii) receipt; (viii) processing; (ix) storage; and (x) disposal. All these stages must be thoroughly observed and documented, especially when concerning digital evidence.

**215.** This reinforces the need to ensure the forensic analysis of evidence obtained by digital means, with the preparation of detailed and thorough expert reports, providing for each stage of the chain of custody, including the need to transfer the evidence and the subsequent storage.

**216.** In conclusion, evidence obtained by spyware, due to the high degree of intrusiveness of the means of proof and the fragility of the information, must be considered to be unlawful or illegitimate if defects are found in the chain of custody. In this case, it is not appropriate to leave these issues to be resolved at the time of evaluation by the Judge, so that **if there is no complete documentation of the chain of custody of the evidence, the digital files obtained should be inadmissible in criminal proceedings.**

## V.4. INDIVIDUALIZATION OF SUBJECTS SUBJECT TO INTRUSION PROCEDURES

**217.** Given the technical capacity of the surveillance tools acquired by the Brazilian government, there is concern as to the possibility of massive investigations, affecting hundreds of individuals without strict criteria to ensure that conduct violates fundamental rights, such as privacy and data protection, within the scope of investigations and intelligence.

**218.** All spyware categories presented here have implications in this regard. Information extraction software, cryptographic key decryption, deletion of files and cloud files indiscriminately collect the electronic devices that are the target of the search, corroborating the risk of a fishing expedition. Without imposing the necessary continence and connection with the crime being investigated, there is a risk of undermining just cause, inciting the persecution of subjects and abuses of state power.

**219.** Also noteworthy is the ability of infrastructure vulnerability exploitation tools to monitor thousands of people. FirstMile, for example, provides a license to monitor 10,000 individuals, and there is no documented proof of the criteria established for choosing such surveillance. In the case of information extraction by inference, the opacity of the criteria used by the algorithms endangers people who are related to the targets of the investigation, further expanding the remote monitoring network.

**220.** Any monitoring measure must necessarily be targeted and limited to the people identified as causing the threat[118]. It is worth noting that under no circumstances could such monitoring violate the core of an individual's intimacy and private life[119].

**118** MENKE, Fabiano. Data protection and the new fundamental right to guaranteed confidentiality and integrity of technical-informational systems in German law. In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (org.). Law, innovation and technology. São Paulo: Saraiva, 2015. p. 224.

**119** MENDES, Laura Schertel. Use of spyware by the police: legal practice? JOTA. Jul. 05, 2015. Available at: https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policiapratica-legal-04062015. Accessed on July 18th, 2024.

**221.** In Brazil, technologies for collecting and processing personal data are used by the Brazilian Intelligence System with no regard for these criteria. Identifying a concrete danger or threat to a fundamental legal interest is essential, as it prevents unfounded and disproportionate monitoring of the population. After all, if you can't identify the danger or threat, what are you investigating? Since there is no specific target that motivates intervention in the integrity and confidentiality of technical and information systems, everyone becomes a target, giving rise to discretionary and arbitrary action by public agents.

**222.** Therefore, it is imperative that the subjects who would be targeted by this measure are properly individualized, along with the unlawful conduct that needs to be investigated. Otherwise, there would be an inexplicable invasion of the lives of those affected and a clear violation of the right to privacy and intimacy. Any possibility of abusive use of these tools must thus be ruled out, with maximum determination of the object of investigation, in order to avoid the configuration of a surveillance State in the midst of a democratic order.

## V.5. THE NECESSARY DEVELOPMENT OF OTHER PARAMETERS COMPATIBLE WITH THE CONSTITUTIONAL ORDER

**223.** The illegality of the processing of personal data by Intelligence and Public Security agencies also lies in the absence of procedural instructions and positive safeguards to promote the proper protection of data subjects. Given the State's vast technological apparatus, citizens are left unprotected, suffering the severe consequences of the invasion of their private lives.

**224.** As previously explained, the infiltration of spyware allows for a much broader data collection than mere telephone or telematic interception, as it is not just about intercepting a specific data traffic, but rather collecting all the data on a certain device that is already stored or being produced in real-time.

**225.** In light of this high degree of interference in human life and the sensitivity of the information that can be collected, in addition to drafting a specific law that legally authorizes the use of spyware by investigative authorities, as well as the presence of judicial authorization, it is also essential to i) identify a concrete danger to a legal asset, in the specific case, besides ii) ensuring the core of intimacy, that

is, whenever extremely intimate information is collected, it must be discarded or protected in a safer way by the police authority.

**226.** In this context, it is important to bring up certain parameters outlined by Dr. Laura Schertel Mendes during a public hearing held within the scope of this ADPF. According to her, the infiltration of devices by the competent authorities using spyware can only occur when i) specific conditions are met, such as ii) a secure legal basis, iii) the necessary clarity regarding the purpose of data processing to assess the level of intervention in fundamental rights, and it must also be iv) proportional, appropriate, and necessary to the intended purpose, while also adopting v) minimal preventive measures of a procedural and organizational nature, aimed at ensuring the safety of the citizens involved and reducing the risks of harm to their personality rights.

**227.** In other words, the more severe the restriction on fundamental rights, the more compelling the justifications, criteria and precautions must be.

## VI. THE REQUESTS

**228.** In light of the above, the *amici curiae*, duly admitted by this Honorable Court to assist in the judgment of the case, request that this Honorable Superior Court **declare the unconstitutionality of the State's use of spyware,** due to the violation of fundamental rights and the context in which they are used, exploiting the vulnerabilities of other platforms where the priority should be the right to the integrity of informational systems.

**229.** **Alternatively,** it is requested that the immediate **suspension** of the use of spyware tools by Brazilian Authorities be ordered **until their use is properly regulated by legislation in the Brazilian Congress.** In this case, it is requested that strict criteria be established for the use of spyware, analogous to the existing regulations for other cases of breach of confidentiality, particularly (i) the requirement of prior judicial authorization and adherence to similar strictness as in other situations of confidentiality breach; (ii) the constitutional interpretation of communication confidentiality updated to contemporary standards of intrusiveness; (iii) the inclusion of mechanisms to respect the chain of custody; (iv) the individualization of subjects subjected to intrusion procedures; (v) the development of other parameters compatible with the constitutional order.

**GRANT IS REQUESTED.**

BRASÍLIA/DF, JULY 29TH, 2024.

Bárbara P. Simão
OAB/SP No. 428.335

Danyelle Reis
CPF No. 111.020.786-70

Francisco Brito Cruz
OAB/SP No. 314.332

André Houang
OAB/SP No. 463.200

Pedro Saliba
OAB/RJ No. 211.334

Vinicius Fernandes da Silva
CPF No. 403.305.468-56

Rafael A. F. Zanatta
OAB/SP No. 311.418

Felipe Fernandes de Carvalho
OAB/DF No. 44.869

Ivan Cândido da Silva de Franco
OAB/SP No. 331.838

Cíntia Anacleto Isawa
OAB/SP No. 451.872

Amanda Boukai Chapaval
OAB/SP No. 508.238

# DOC 1

# Typologies by State

INTERMEDIARY Grupo TechBiz — MANUFACTURER Cellebrite — 8 DIFFERENT TECHNOLOGIES

### DECRYPTION OF CRYPTOGRAPHIC KEY

- Unlocking devices protected by pattern, password or PIN code;
- Encryption bypass on Android and iOs devices;
- Data recovery from other applications such as WhatsApp, Face book and Telegram; Access to emails and attached files;
- Access to geolocation data from cell and Wi-Fi towers;
- Partial data extraction even when the device is locked;
- Bypassing or determining passwords on all major Samsung devices;
- Access to data from applications protected with an additional password via KNOX;
- Screen unlock by pattern, PIN code or password on the latest iOS and Android devices;
- Automatic pin-out recognition.

### EXTRACTION OF DELETED INFORMATION

- Logical and physical extraction from cell phones, drones, SIM and SD cards, GPS devices and others, including extraction of the entire file system (full file system extraction) or selected files according to the application;
- Visualization, categorization and systematization of backups made via data extraction from UFED, including encrypted data.

### EXTRACTION ON DEVICE

- Recovery of deleted files;
- Data extraction from devices based on Qualcomm chipsets, regardless of manufacturer (function for UFED 4PC);
- Application emulation to visualize extracted data in its original format;
- Unlocking Apple devices on the latest versions of iOs;
- Minimizing attempts to unlock using brute-force techniques to reveal passwords;
- Full-file system extraction from iOS devices, including encryption bypass of iTunes backups;
- Access to stored passwords and Keychain tokens (password management system in macOS);
- Physical extraction and decryption of data from mobile devices, including full-file system extraction from iOS and Android devices;
- Physical extraction of existing, hidden and deleted data from Chinese-made cell phones;
- Extraction of user passwords.

### CLOUD COMMUNICATION SYSTEM EXTRACTION

- Gaining information on an individual's intentions, interests and relationships by analyzing posts, likes and connections;
- View a user's activities and locations from Facebook, Google and iCloud across multiple devices;
- Features based on machine learning algorithms and pattern recognition, correlating media files, contact analysis and interactions with third parties to define who, what, where, when and why;
- Monitoring the use of other data extraction and analysis tools;
- Distribution and remote installation of software updates and configuration changes.

### SECOND-ORDER INFORMATION EXTRACTION

- Extraction and analysis of cloud-based content available in more than 50 cloud applications and sources;
- Access to data no longer stored on physical devices when recovering cloud backups.

### OTHER

- Visualization of correlations and connections about an individual from different data sources;
- Secure Folder (Galaxy's data encryption feature);
- Extraction of unallocated data to maximize recovery of deleted items;
- Recuperação de dados de outras aplicações como Whatapp, Facebook e Telegram;
- Access to emails and attached files;
- Access to geolocation data from cell towers and Wi-Fi;
- Recovery and examination of data on crushed, broken, burnt or water-damaged devices;
- Automatic collection of usage statistics from other tools;
- Automatic metadata backup of all data extractions;
- Storing usage activity logs with analysis panel.

INTERMEDIARY Grupo TechBiz — MANUFACTURER opentext™ — 2 DIFFERENT TECHNOLOGIES

### DECRYPTION OF CRYPTOGRAPHIC KEY

- Access to encrypted data with Bitlocker (Windows 10), Data Protection 8.17 (Dell) and PGP v10.3 (Symantec);
- Password bypass to recover images from locked Android systems, such as Samsung, Motorola, LG, MTK, and Qualcomm, with advanced extraction capabilities;
- Its manufacturer, Magnet Forensics, has partnered with Passware, providing examiners with the ability to retrieve data from drives encrypted with TrueCryt and BitLocker.

### CLOUD COMMUNICATION SYSTEM EXTRACTION

- Recovery of data and communications from applications with cloud storage, such as WhatsApp, Facebook, Instagram, Google, Twitter and others;
- Filtering, tagging and viewing conversations for individual messages and full chats.

### SECOND-ORDER INFORMATION EXTRACTION

- Computer, cell phone, cloud and car support;
- Image recognition, including faces and objects;
- Support for analyzing data extracted from devices from other tools.

### OTHER

- Acesso a dados encriptados com APFS (Apple File System);
- Bypass da segurança para o Apple T2.

INTERMEDIARY Grupo TechBiz — MANUFACTURER exterro — 1 TECHNOLOGY

### DECRYPTION OF CRYPTOGRAPHIC KEY

- Search browsing history of all browsers and segmentation by metadata category (adult content, chats, dark web, news, etc.);
- File decryption, password cracking; password recovery for over 100 applications;
- Decryption of encrypted computer disks with the latest version of McAfee Drive Encryption.

### EXTRACTION OF DELETED INFORMATION

- Collecting, processing and analyzing data sets containing encrypted, compressed or deleted Apple system files;
- Decrypts FileVault 2 from the APFS (Apple File System) file system;

### CLOUD COMMUNICATION SYSTEM EXTRACTION

- Recovery of data and communications from applications with cloud storage, such as WhatsApp, Facebook, Instagram, Google, Twitter and others;
- Filtering, tagging and viewing conversations for individual messages and full chats.

### SECOND-ORDER INFORMATION EXTRACTION

- Database unification for storing evidence; Indexing, filtering and search tools for stored data results;
- Image recognition and detection, including faces and objects;
- Location, handling and filtering of data, mobile, network, with segmentation between data and communications.

INTERMEDIARY apura — MANUFACTURER MSAB — 7 DIFFERENT TECHNOLOGIES

### DECRYPTION OF CRYPTOGRAPHIC KEY

- Access and analysis of data in applications with strong encryption, such as WhatsApp, WhatsApp Business and Telegram and Signal;
- Compatible with Android devices;
- Possibility of accessing data from blocked cell phones;
- Reconstruction of deleted files.

### EXTRACTION OF DELETED INFORMATION

- SIM card cloning;
- SIM card reading and cloning;

### EXTRACTION ON DEVICE

- Extracting and copying data from digital devices, including SIM and SD memory cards;
- Physical extraction of data from mobile devices;
- Password bypass and/or recovery
- Extracting data from digital devices;
- Logical and physical extraction of data from mobile devices, including deleted data.

### CLOUD COMMUNICATION SYSTEM EXTRACTION

- Data extraction from applications with cloud storage, such as Facebook, Google, iCloud, Twitter and Snapchat. Includes automatic extraction mode, from application access tokens previously extracted with the device in hand, and manual extraction, with no need for the device to be present, from login and password previously accessed by other means.

### SECOND-ORDER INFORMATION EXTRACTION

- Adds visualization features to XAMN Spotlight, such as analysis based on geolocation, conversations in messaging applications and connections between different users and different devices;
- Analysis, filtering, visualization and systematization of data extracted from mobile devices, drones, wearable technologies, GPS, vehicles, SIM cards, memory cards and other sources.

### OTHER

- Recognizing content in images;
- Support for extracting and decoding data from "non-standard" devices ("typically manufactured in Eastern Asia");
- Automatic identification of pin-outs; Support for MediaTek, SpreadTrum, Coolsand and Infineon chpsets;
- Extracting data from GPS devices.

INTERMEDIARY apura — MANUFACTURER exterro — 1 TECHNOLOGY

### DECRYPTION OF CRYPTOGRAPHIC KEY

- Browsing history from all browsers and segmentation by metadata category (adult content, chats, dark web, news, etc.);
- File decryption, password cracking; password recovery for over 100 applications;
- Decryption of encrypted computer disks with the latest version of McAfee Drive Encryption.

### SECOND-ORDER INFORMATION EXTRACTION

- Unified database for storing evidence;
- Indexing, filtering and search tools for stored data results;
- Image recognition and detection, including faces and objects;
- Location, handling and filtering of data, mobile, network, with segmentation between data and communications;

### OTHER

- Collecting, processing and analyzing data sets containing encrypted, compressed or deleted Apple system files;
- Decrypts FileVault 2 from the APFS (Apple File System) file system.

INTERMEDIARY Cognyte — MANUFACTURER Cognyte — 3 DIFFERENT TECHNOLOGIES

### DECRYPTION OF CRYPTOGRAPHIC KEY

- Interception of calls and text messages;
- A5/1 and A5/2 encryption breaking, with built-in decoder.

### INFRASTRUCTURE EXTRACTION

- Precise location of the target device using a dedicated homing device, without disabling the target from communicating;
- Extraction of GPS coordinates from the target's cell phone on GSM and UMTS (3G) networks;
- Collecting GSM traffic in a "wide area"
- Identification of "suspicious communication patterns" based on location, speech recognition, link analysis and correlations between texts;
- Allows monitoring of up to 10,000 cell phone owners every 12 months.

### OTHER

- Listen to, read, edit and redirect incoming and outgoing calls, as well as text messages (A5/1 and A5/3 encryption);
- Remotely activate a cell phone's microphone;
- Identify the presence of the target's handset;
- Block cellular communications to neutralize IEDs and more;
- Intercept incoming and outgoing SMS;
- Allows multiple users to analyze calls at the same time;
- The technology locates devices using 2G, 3G and 4G networks. Through flaws in the Signaling System No. 7 (SS7) protocol, which should only be shared between telecom providers for roaming;
- Identifying the approximate location of devices, generating alerts about the routine movement of targets of interest.