weizenbaum journal OF THE DIGITAL SOCIETY

05 ISSUE 02

WEIZENBAUM JOURNAL OF THE DIGITAL SOCIETY
Volume 5 \ Issue 2 \ w5.2.3 \ 06-10-2025
ISSN 2748-5625 \ DOI 10.34669/WI.WJDS/5.2.3

Information on this journal and its funding can be found on its website:
https://wjds.weizenbaum-institut.de

KEYWORDS

intelligence oversight
Brazil
Germany
government hacking
democracy

RESEARCH PAPER

Democratic Oversight of Government Hacking by Intelligence Agencies

A Critical Analysis of Brazil and Germany

André Ramiro

Universität Hamburg, Germany
andrebramiro@gmail.com

ABSTRACT

Regulating intelligence services is a challenge for modern societies worldwide. Their very *modus operandi* relies on tight secrecy protocols for the information gathered, internationally and domestically. Evolving surveillance techniques include exploiting the vulnerabilities of digital services, dealing on unregulated surveillance markets, and developing tailored tools. Theoretically, these actions aim at the public interest by, for instance, anticipating terrorist attacks or dismantling pedophilia networks. Nevertheless, they are increasingly used to surveil civil society without proper and demonstrated necessity or proportionality. Given the demand for increased transparency and accountability for intelligence agencies, especially when using hacking technologies, what institutional design and civic participation avenues for oversight may be proposed? How can (existing and yet-to-exist) institutions improve democratic external oversight activities in this realm? Through a comparison of Germany's and Brazil's legal frameworks and institutional ecosystems, the paper critically explores the meaning of "democratic oversight" of intelligence agencies, specifically observing oversight models for hacking operations. Looking

at previous contributions by intelligence studies scholars in these countries and globally, the paper offers a critical-comparative analysis of institutional and political architectures to assess the levels of democratic participation. On this basis, it makes recommendations for both countries, which can be appropriated by external intelligence oversight bodies.

1 Introduction

Historically, information about state intelligence activities has been covered by secrecy protections normally grounded in national security interests. The notion that a certain level of secrecy is necessary to safeguard sensitive government information on domestic and global scales gives rise to a transparency problem: the necessity invoked by intelligence agencies may appear unjustified in the public's eyes, and civil society can become skeptical about activities that involve gathering information about civilians, political movements, private companies, and other states. The ensuing transparency dilemma thus consists in balancing intelligence effectiveness with public transparency (Zegart, 2000; 2011; Cepik, 2023; Wetzling, 2023b) to achieve a regime of accountability (McKune & Deibert, 2017; Kaye, 2021) through an ecosystem of democratic oversight.

The topic of hacking activities by these agencies is even more dynamic and insufficiently addressed in public policies. The historical and cultural lack of external intelligence oversight is often connected to intelligence practices that are technically complex and advanced, such as hacking procedures. Furthermore, government hacking activities may rely considerably on private international vendors, whose technologies do not allow sufficient transparency over their functions and development (Council of Europe, 2023; Ramiro et al., 2022). These vendors rely on a "legitimate" status as they have governments as their primary customers, making them difficult to regulate through domestic and international efforts (Anstis, 2021). As will be discussed in this paper, some developments have occurred in national and international regulatory landscapes through governmental measures and civil society and litigation initiatives against spyware companies and intelligence laws (Kniep et al., 2023; Schneier & Penny, 2022; Knight First Amendment Institute, 2022).

Government hacking has been discussed as a major privacy and security problem in recent years. On the heels of the encryption debate (Gasser et al., 2016), some authorities have turned to searching for existing vulnerabilities in information systems. The bright side of this approach is that a more "tailored" surveillance apparatus could be achieved (Bellovin et al., 2014) instead of coercively inserting mandatory vulnerabilities, such as backdoors, in the communication platforms and devices used by the bulk of citizens (Abelson et al., 2015). At first

sight, this would supposedly make for a less problematic and more proportional solution. Nevertheless, the ripple effects are numerous. For instance, it may lead to the expansion of the international spyware industry and for this industrial circuit to negotiate with autocracies[1] that monitor thousands of journalists, activists, political dissidents, and public authorities, deepening human rights violations on a global scale (Citizen Lab, 2024; Forbidden Stories, 2024). As in the Vault 7 case (Wikileaks, 2017), governments can also lose control of these technologies, which either fall into the hands of criminal actors or are used by public authorities for personal and political purposes (Newman, 2024). As a consequence, security researchers may be motivated not to disclose vulnerabilities to the original vendors but rather to private brokers, resulting in greater incentives for spyware makers from the market or governments (Pfefferkorn, 2018).

To offer a legal and political comparison that can contribute to improvements in the oversight of hacking operations by intelligence agencies, this paper takes Germany and Brazil as initial case studies. Germany has made considerable progress in public debates concerning the exploitation of vulnerabilities by public authorities. This has led German parliamentarians to play an active role in the recent "Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware" (PEGA), an inquiry pursued by the European Parliament (2023) regarding the impacts of the Pegasus spyware in the region. Furthermore, as early as 2008, the German Federal Constitutional Court (Bundesverfassungsgericht, BVerfG) established the "fundamental right to the confidentiality and integrity of information technology systems" (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*), also known as the "IT right," in a landmark ruling that has since shaped contemporary policies in the country (Schafer & Abel, 2010; Menke, 2019). Other rulings over the last years have also addressed privacy and security safeguards for the use of hacking tools by public authorities. The role of civil society organizations (CSOs) in Germany has been also fundamental in fostering the public debate, notably through landmark litigation cases (Kniep et al., 2023; Hummel et al., 2022). These decisions have led to more procedural requirements, oversight mandates, and reforms to several laws regulating intelligence agencies' work and law enforcement.

---

[1] As well as Western democracies. See the takeaways from the panel "Digital Authoritarianism on the Open Market," hosted by the Atlantic Council's Digital Forensic Research Lab: "These tools are open for misuses, not just by different authoritarian governments, but also by democracies worldwide… Some spy tech programs have been successfully exposed. Milan-based Area Spa was raided by Italian authorities in 2016 after being accused of working with Syria. Munich-based FinFisher was raided by German authorities in 2020 after its tech was used by the Turkish government and others, and has since shut down." For more, see Fouriezos (2022).

In Brazil, the topic has gained attention in recent years, especially under the Bolsonaro administration. Studies have provided an overview of the state of government hacking in the country (Ramiro et al., 2022; Dutra et al., 2023), and CSOs and political parties have fought human rights violations through advocacy and litigation efforts before public authorities. For instance, the Brazilian Federal Supreme Court (*Supremo Tribunal Federal,* STF) recently decided on the unconstitutionality of data sharing among intelligence services without specific due process, and the Brazilian Intelligence Agency (*Agência Brasileira de Inteligência*, Abin) is currently under investigation by the Federal Police for illegally monitoring journalists, parliamentarians, and even members of the executive branch by exploiting vulnerabilities in the telecommunication system. This political case will be the starting point for a constitutional lawsuit before the STF pointing out the lack of regulation for such activities.

The proposed comparison between both countries is even more relevant to fostering the accountability of their intelligence services when viewed through a historical lens. For example, the personal communications of both heads of state were monitored by the National Security Agency of the United States, one of the key revelations from Snowden's disclosures (Ball, 2013). A legal and institutional comparison of these two countries is justified for several reasons. First, it offers the opportunity to translate legal cultures and frameworks, triggering international understandings and improvements concerning fundamental rights and institutional designs, especially against the backdrop of these two countries' adoption of the "Right to privacy in the digital age" resolution addressed to the United Nations General Assembly after the Snowden revelations (United Nations, 2013). This adoption can serve as a point of reference regarding how these countries have addressed surveillance policies by looking at their current intelligence oversight systems. Second, Brazil and Germany have a history of comparative legal studies and participation in each other's academic networks on Internet regulation. Third, the topic has a fundamentally international layer and requires multilateral understandings, agreements, and political relations. Comparing these two scenarios offers an intercontinental reflection on their political organizations and socioeconomic realities. Lastly, while Germany has a profound history of public debate and legislation on privacy and data protection, Brazil is globally recognized for its multistakeholder approach to Internet governance. Therefore, given that oversight of hacking operations is a tangible aspect of Internet regulation, the topic is connected to the rules governing digital communications and infrastructures, which include the politics around the exploitation of vulnerabilities. Therefore, both countries can benefit from the discussions proposed here, which help to assess the effectiveness of risk control and the accountability of intelligence services and hacking operations.

To systematize the comparison between the two countries, the paper explores their legal vocabularies for hacking activities by intelligence services and describes the institutional design of external intelligence oversight of both countries (i.e., centralized or distributed). In addition, it examines the problems and merits of specialized and political oversight according to the literature in the field and the degree of openness to civic participation through institutional and non-institutional venues. To refine the intelligence oversight vocabulary and hacking techniques typology, the paper investigates how to better frame what is meant by "democratic oversight" and "government hacking" based on current legislation, political theory, and intelligence studies. The next section describes the current status of external oversight activities in Germany and Brazil as concerns intelligence agencies, the related legal frameworks in both countries, and their relations to the expanding use of hacking tools, exploring best practices according to the existing literature. Next, we propose improvements in both countries to open democratic avenues for greater transparency and accountability in the use of hacking tools by intelligence agencies.

Finally, although proper semantics are needed, the regulatory nature of the discussion must, to some extent, remain flexible, meaning that regulatory debates should be relatively open to allow for updates in order to keep up to the state of the art in cybersecurity and human rights patterns. Additionally, democratic oversight models require an ecosystem of authorities instead of a single one, as well as strong venues for public participation. Further, given the cross-border nature of the activity, its social impacts, the public authorities behind it, and the industry involved, domestic and international efforts must be combined.

2 A Semantic Framework for Democratic Oversight and Government Hacking

Oversight broadly refers to "an actor scrutinizing an organization's (or individual's) activities with the aim of evaluating its compliance with particular criteria and on this basis, issuing recommendations or orders to the organization concerned" (Wills & Vermeulen, 2011). The "democratic" aspect of oversight can be approached from multiple angles, but we anchor it in modern concepts of social justice and the public sphere – concepts fundamentally attached to theories of democracy and political philosophy – together with contemporary debates put forward by intelligence and surveillance studies scholars.

Proposing an initial semantic framework for these activities, Roller et al. (2023) categorize, two subsets of oversight models: a *delegated* model, where "external bodies are bestowed with legal oversight mandates and powers by the state," and a civic model, which "by contrast, refers to the scrutinizing practices by the media, CSOs, and citizens who complement delegated over-

sight through an oftentimes more adversarial and more public mode of oversight."[2] As oversight system failures revealed the existence of mass surveillance programs—from Snowden's revelations to Wikileaks' Vault 7 and the broad use of spyware by governments around the world – recent studies have argued that another way to define the concept of democratic oversight is to address the struggles faced by CSOs in the "real world."[3] Based on the oversight performed by CSOs, Kniep et al. (2023) attribute at least three elements to democratic oversight: advocacy, activism, and litigation. These act as *de facto* forms of oversight of intelligence activities, "non-official" venues, and, at the same time, ways of challenging traditional notions of what "democratic" means in oversight activities.[4] The authors argue that "liberal, functionalist, and technocratic views" of intelligence oversight studies limit the range of democratic and "radical transparency" (Kniep et al. 2023, p. 2010) practices, such as whistleblowing.

In terms of effective transformative policies leveraging the power of the public, activating oversight bodies and, more broadly, public institutions to protect collective rights (such as policymakers, courts of justice and audit, public prosecutor's offices, or data protection authorities) is one of the ultimate objectives of advocacy and, especially, litigation efforts. The "complementary" aspect of civic oversight connects to Habermas's (1992) thesis of "co-originality": the circular process of legal form and democratic participation, - seen in interactions between public institutions and civic political activities that are fundamental to the making of politics in the public sphere, which depends on the connection between contestatory praxis (typical of civil society work) and the institutional rationality and process of decision-making. Far from the individual and liberal aspect of privacy seen in historical theorizations, the private sphere elaborated by Habermas is intrinsic to the communicative infrastructure part of transformations of political systems, their agendas, and routines of functioning (Silva, 2021). Drawing on Habermas's notion of political engagement, Cohen and Fung (2021) argue that these two tracks – *civic* and *official* – are complementary to democracy and, thus, depend on integrating

---

2 I would add that for the first category, the framing is for specific bodies other than *organic* judicial and administrative control over intelligence activities, such as courts of justice and audit. The notion of *specialized oversight* bodies in the work of Wills and Vermeulen (2011) also contributes to this consideration.

3 Interestingly, theoretical and practical problems are seen as diffuse. In the realm of encryption studies, the symposium "Real-World Cryptography" defends a similar point of view: "the conference goal is to strengthen the dialogue between these two communities [developers and researchers]. Topics covered focus on uses of cryptography in real-world environments such as the Internet, the cloud, and embedded devices" (Real World Crypto Symposium, 2024). Commenting on the *motto* of the symposium, Philip Rogaway (2015) states that "as academics gravitated to cryptography, they tended to sanitize it, stripping it of ostensible connectedness to power. Applied and privacy-related work drifted outside of the field's core venue… It is as though a chemical synthesis would take place, transforming this powerful powder into harmless dust." This also seems to be a problem with intelligence oversight studies.

4 The concept of *sousveillance* elaborated by Mann, Nolan, and Wellman in 2003 contributes to the academic archaeology of theories about "watching the watchers," "inverse surveillance," or, more broadly, "reporting on authorities." Julie Cohen (2019) also highlights the history of legal *counter-movements* that defy injustices. Although "inevitably temporary… they disrupt the rhetorical and institutional logics that power has constructed" (p. 270).

public discussion fueled by informal/peripheral communications with formal decision-making entities. Therefore, they are centrally linked to the openness of the public sphere.[5] And even though they may not always be open to all interested parties, eventual blocks to participation feed the political potential for contestation against traditional institutions and practices (Silva, 2021).[6] I argue that this paradigm of co-originality applies not only to the realm of intelligence oversight but also to any contestatory praxis related to institutional-political arrangements that struggle for participation and recognition. Even so, the realm of intelligence oversight deals with structural and visible loopholes that make it specially relevant for analyzing how it fits – or does not fit – within democratic regimes, highlighting its contemporary pertinence.

Meanwhile, security and legal scholars have reported on and conceptualized developments like hacking activities by public authorities over the last 10 to 15 years. Hacking procedures have been described using a variety of terms, from *lawful hacking* (Bellovin et al., 2014; Hennessey, 2016) or law enforcement hacking (Quinlan & Wilson, 2016) *to equipment interference* (Big Brother Watch, 2016), *state trojans* (Buermeyer & Mioni, 2018), or *computer network exploitation* (Wetzling, 2017). Here, we adopt the definition of government hacking as discussed by Ramiro et al. (2022), the exploitation of vulnerabilities by public authorities, known or unknown by the original vendor, which results in non-authorized access to data or communication, at rest or in transit, with the intention of gathering such information by working around a security system. As a matter of scope, however, we analyze specifically the institutional circuit of oversight of hacking procedures by intelligence agencies. Additionally, this definition resonates with an approach to "cyber-incidents" based on the actor-network theory adopted by Balzacq and Cavelty (2016, p. 180) as "deliberate disruptions of routine and everyday cyber-security practices, designed to protect networks, computers, programs and data from attack, damage, or unauthorised access," with the addition that public institutions are the actors of these disruptions. Finally, we refrain from using the term "lawful," first because the current debate around legality parameters is far from being resolved, and second because these activities are often performed in a deliberate departure from fragmented views of legality to escape transparency and accountability, as in autocratic regimes, a phenomenon already framed as "autocratic legalism" (Scheppele, 2024).

---

5 Although this is not within the scope of this paper, it would be possible to contest the potentiality of political engagement by both civil society and policymakers (both affected, even though not equally) with regard to the irreparable effects of surveillance practices and privacy violations.

6 Participation in the public sphere can be seen as a consequence of the recognition of the many communities in a society and their political representation within – but not limited to – institutionalized bodies. The development of the three-dimensional theory of justice by Nancy Fraser (2008; Cyfer & Neves, 2011) has emphasized representation as a central pillar of just democracies, involving communities long unrecognized in political arenas, including the governance of institutions and their subject of competence as a locus of social justice. As a result, the venues for participation within the circuit of intelligence oversight mechanisms, whether civic or delegated, are an important matter of recognition and representation, rationalities from which social demands can propose continuous scrutiny and redefine expectations over intelligence activities.

These terminologies are more established and codified in laws concerning criminal and intelligence procedures. As developed in detail below, the BVerfG has ruled in several cases that authorities have to follow legal obligations based on legality, proportionality, and necessity and qualify the oversight mechanisms for covert surveillance routines. As a result, at least two different typologies for exploitation techniques are seen in the jurisdiction: "telecommunications surveillance at the source" (*Quellen Telekommunikationsüberwachung*),[7] comprising the interception of encrypted private communications at the device-end, and "online search" (*Online Durchsuchung*), more pervasive techniques not limited to collecting encrypted communications in plain format but also encompassing data from other sources, such as cloud services and the device's hard drive. Additionally, the German Parliament (Deutscher Bundestag, 2022) clarified two aspects that are crucial to understanding the technique and its possible lawfulness. First, these procedures must be balanced against the fundamental right to the confidentiality and integrity of information technology systems, which derives directly from the fundamental right to the free development of personality and human dignity. Second, there is a difference between the use of hacking technologies by law enforcement and by intelligence agencies, pointing out the legal regime and specific due process for each branch, which endorse the principle of informational separation of powers (*informationellen Trennungsprinzips*; Ruschemeier, 2022; Sarlet & Sarlet, 2022). This entails avoiding, for example, a "common database" for different government bodies, which may result in the formation of a "secret police."[8]

In Brazil, hacking tools, though embedded in investigative culture in recent years (Ramiro et al., 2022), are used *by analogy* to other typical investigative techniques and are thus subject to traditional rules regarding, for example, *infiltration* or *interception*. However, the exploitation of vulnerabilities does not fit into known categories and is, therefore, an *atypical* technique. Nevertheless, the legal debate around the analogous application of atypical investigative techniques is far from resolved, especially when serious violations of fundamental rights are at stake. To criminal procedure scholars in Brazil, such as Badaró (2012) and Greco Filho (2012), the analogy may apply when the

---

7 There would be a third type of technique, the so-called "Quellen TKÜ Plus." The difference between them both would be that the "Plus" extends prior to the date of the judicial authorization, making possible the collection of stored communications, while the "regular Quellen TKÜ" only applies from the date of the judicial authorization in order to collect on-going communications. Critiques of the Quellen TKÜ Plus can be seen in Kurz (2023), stating that the "Plus" version amounts to "online search".

8 The principle is better elaborated on by the German Federal Constitutional Court (Bundesverfassungsgericht, 2013) in a case (BvR 1215/07) concerning the "Antiterrorism Files Act" that created a "joint files database," which was declared unconstitutional by the court in 2013. According to Ruschemeier (2022) "[t]he police and intelligence services are officially separated from each other. This separation requirement is based on the different areas of responsibility and competencies of both institutions. The organizational-administrative (no joint authority, no secret police or secret service with police powers) and personnel separation (no joint employment of officials) are the overwhelming consensus… The consequence of this differentiation is that data processing is also subject to different specifications, and the technical and federal separation thus has fundamental rights relevance for data protection. This leads to the principle that no joint data exchange between the police and intelligence services is permitted."

technique is atypical, but it must follow restrictions based on legality, judicial control, and the dignity of the human person. Although analogies within criminal procedure are possible, according to the Brazilian Institute of Criminal Sciences (Instituto Brasileiro de Ciências Criminais, 2009) atypical techniques have to follow legally determined procedures. Thus, the question remains: Can the legality of the use of hacking techniques be fulfilled by analogous procedures based on other surveillance measures?

Badaró (2012) points out the consensus among Brazilian criminal procedural scholars that there is no need for a rigid definition of typologies of investigative techniques for the production of evidence – that is, they favor a broader approach to the atypicality of evidence. However, atypical techniques must obey certain restrictions, such as human values and reasonability. In addition to terminology and typicality, the (il)legality of the evidence may also be pertinent. For Greco Filho (2012), this may support the inadmissibility of evidence obtained through illegal means, as established by Article 5, LVI, of the Brazilian Constitution.[9] Accordingly, the fact that the exploitation of vulnerabilities is turned into a business model by private agents and marketed to state actors may arguably make any evidence acquired through these means illegal. The "Cybercrimes Law" in Brazil (No. 14,155/2021) typifies the hacking of someone else's device as a criminal activity, including the act of selling computer programs for exploitation. Therefore, for the sake of argumentation, even if a crime is admitted for investigative or intelligence purposes (confronting us with a fine line of legality that can nullify the evidence obtained), it is necessary to emphasize the constitutional principle of the impossibility of illegality in obtaining evidence, including "analogous" uses of other techniques in the procedure. Recently, for example, the Brazilian Superior Court of Justice ruled for the inadmissibility of evidence collected by mirroring a WhatsApp client "as an analogous" technique of regular interceptions (Superior Tribunal de Justiça, 2021).[10] By principle, analogies in the criminal procedure are, as a result, limited.

Establishing new terminologies and specific legal procedures contributes to assessing the risk and necessity of hacking technologies that exploit security breaches and may suspend fundamental rights. The terminological debate between the types listed above, even in the case of an analogous interpretation of criminal process and intelligence law, involves considerably different modalities that require unprecedented risk assessments, counterbalancing the effectiveness of the intelligence activity and novel considerations of proportionality. Virtual infiltration, interception of telecommunications, or environmental bugs are far from the invasiveness of sophisticated *zero-click* malwares (i.e., spyware that infects a device without requiring a single action from the

---

9 Art. 5, LVI: It is inadmissible, in the process, evidences acquired by illicit means (my translation)

10 According to the Court's ruling, "the measure could not be equated to telephone interception, as this allows listening only after judicial authorization, while mirroring allows the investigator unrestricted access to previously recorded conversations, and can even actively interfere in the exchange of messages between users" (Superior Tribunal de Justiça, 2021) (my translation).

user, not even a click on a malicious link) such as Pegasus used to obtain data on a protected hard drive or cloud service. From a public authority behavior perspective and in reference to the system of fundamental rights protection, a "legal gap"[11] separates traditional techniques from the exploitation of vulnerabilities: a cell phone, with its numerous applications, contains much more information and potential rights' violations than the suspension of the secrecy of telecommunications, for instance.

Two scenarios emerge as a result: one with proper typologies and another with an analogous application of traditional investigative methods to contemporary hacking-based surveillance tools. Therefore, the German legal landscape currently relies on specific legal provisions and investigative procedures for the use of hacking tools, while the Brazilian legal frameworks are still anchored in outdated provisions concerning other traditional techniques. As remarked by the European Parliament's (2023) PEGA Committee Recommendations and echoed by international regulatory proposals made by Kaye (2021) and McKune and Deibert (2017), the lack of a solid legal framework including safeguards, oversight, and a proper technical grammar considerably increases the risks of abuse.

Still, emphasizing a nuanced conclusion is necessary: although establishing a proper semantic framework for hacking routines is one of the first steps towards ensuring that intelligence services respect the rule of law, from a regulatory perspective these categories might become outdated when new techniques emerge at the intersection of digitalization and state surveillance. At the same time, considering the asymmetrical power relation between citizens and government bodies, new interpretations of fundamental rights might develop to guarantee checks and balances regarding the protection of personal data, social security, and cybersecurity, among others. Thus, the semantic framework of the law must remain sufficiently adaptable and open – while avoiding arbitrariness – to assess the protection of fundamental rights.

[11] There is a debate around the notion of "legal gap" in the interpretation of the law, which denotes the absence of a rule in a legal system and, as a result, a potential moment for shaping the law. Some argue that this moment should not be looked at merely as a "problem" but should also be considered an opportunity for improvement (Astofoli, 2017). Analyzing hacking procedures through the lens of this heuristic dichotomy is useful to our discussion.

3 Reflecting on Architectures of Intelligence Oversight

3.1 The Case of Germany

Two main scales can help analyze how democratic oversight institutional designs are. The first is how justice can be accessed before institutions that have a mandate to establish legal control mechanisms, such as the German courts of justice and courts of audit. The second is the effectiveness of government bodies with specific mandate to oversee intelligence activities, which also conduct *ex-ante* legality assessments and ratify or contest them *ex-post*. Below, we will focus on the second category but also refer to the first one to explore civic participation as a contestatory effort.

Drawing on Wetzling (2023b), we identify three public agencies that conduct intelligence activities at the federal level in Germany: the Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*, BfV) for domestic intelligence, with one office at the federal level and one office for each of the 16 states and whose duties include upholding the democratic order, safeguarding industrial secrets, and conducting counter-intelligence; the German Federal Intelligence Service (Bundesnachrichtendienst, BND) for foreign intelligence, which gathers information about international threats and collaborates with foreign intelligence agencies; and the Federal Office for the Military Counterintelligence Service (*Bundesamt für den Militärischen Abschirmdienst*, BAMAD), the military agency responsible for intelligence gathering for military purposes, such as counter terrorism and extremism. Although not the focus of this paper, other federal law enforcement and military institutions also conduct intelligence work based on surveillance technologies. These include the German Armed Forces (Bundeswehr) and the German Federal Criminal Police Office (*Budeskriminalamt*, BKA). As Wetzling (2023b) notes, some overlap exists, for example, between the intelligence surveillance conducted by the BND and the Bundeswehr, with the former operating without a solid legal framework to ground these activities.

Building on the notion of delegated oversight bodies, the German institutional design is composed of (for the most part) four public authorities: the G10 Commission, the Parliamentary Oversight Panel (*Parlamentarisches Kontrollgremium*, PKGr), the German Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*, BfDI), and the newly created Independent Control Council (*Unabhängiger Kontrollrat*, UKR). The G10 Commission is the control body responsible for authorizing and overseeing requests for suspension of the right to the secrecy of telecommunications (Article 10 of the German Federal Constitution) and is empowered with a judicial mandate – therefore, it has *ex-ante*

and *ex-post* capabilities.[12] The commission is composed of a chairman, four assessors, and five deputies appointed by the PKGr and confirmed by the Federal Government. G10 Commission members do not have to be part of the German Parliament, and their mandate lasts until the end of the legislative term. The Commission must report to the Parliament annually on its activities and decisions.[13] Meanwhile, beyond appointing the members of the G10 Commission, the PKGr is also responsible for scrutinizing the work of intelligence agencies at the federal level. The Panel can demand the submission of detailed information by the federal government regarding federal intelligence agencies' general activities and operations of particular importance. The BfDI, under the Federal Ministry of the Interior, Building, and Community, has an *ex-post* administrative oversight mandate to assess intelligence activities with respect to the legal framework for data protection at the regional and national levels. The BfDI can audit intelligence bodies *ex officio* and as a result of complaints by civil society. The BfDI must also publish annual reports about its activities (Bundesbeauftragter für den Datenschutz und Informationsfreiheit, 2024).

The UKR was created after a 2020 Constitutional Court decision (BvR 2835/17), which ruled that the BND did not have adequate supervision.[14] The UKR's mandate is to oversee foreign intelligence activities, especially *signals intelligence* (SIGINT) and the exploitation of vulnerabilities, as well as collaborations between the BND and foreign intelligence agencies. The council has *ex-ante* and *ex-post* powers, including a judicial mandate and the prerogative to access and audit all BND information systems and activities. To do so, it is designed to have a complementary format encompassing a *judicial* and an *administrative* body, the former composed of two chambers of three federal judges each, elected for a term of twelve years, and the latter responsible for the subsequent "review of facts." Unlike the G10 Commission and the BfDI, the UKR does not have to report its activities to the general public, but it must share reports with the PKGr.[15] Germany has therefore developed a distributed model of intelligence oversight.

---

[12] It is important to highlight that, before the 2016 intelligence legislation reform, foreign-to-foreign SIGINT surveillance activities by the BND were not subjected to any independent oversight, either parliamentary, judicial, or by the BfDI (Wetzling, 2017).

[13] Furthermore, the Commission's supervisory powers extend to the entire procedure of gathering, processing, and using the personal data obtained through restrictive measures, which includes the decision to inform the targeted individuals or not. In this context, the Commission can demand information, inspect files, and have physical access to all offices. See detailed information in Bundesamt für Verfassungsschutz (2024).

[14] According to the literature on intelligence studies in Germany, the ruling was a landmark decision: it not only asserted the inadequacy of BND oversight by then, but also held that the fundamental rights of German nationals apply to non-citizens abroad when surveilled. See the decision in Bundesverfassungsgericht (2020) and the interpretations in Reinke (2020) and Gesellschaft für Freiheitsrechte (2020).

[15] About the 2020 Constitutional Court decision, Kniep et al. (2023) describes how intelligence officials publicly disqualified the plaintiffs during the case calling them "fools" and how, even after the landmark ruling, the BND managed to pass an amendment to its regulatory law, the BNDG, to provide hacking powers to the agency. Kniep (2024) also underlines the systemic problems of silencing and symbolic power concerning the practice of the Third Party Rule, a code of conduct among intelligence agencies in the context of international cooperation.

In addition to institutionalized oversight, the scrutiny and constant efforts conducted by CSOs in the country have fundamentally shaped the debate and provoked necessary reforms concerning intelligence activities. For reasons of scope, we discuss only a few cases of litigation before the BVerfG as venues in which civil society has contested the constitutionality of intelligence practices in the realm of exploitation of vulnerabilities. First, the 2008 landmark ruling within the constitutional complaint BvR 370/07, which established the constitutional "right to the integrity and confidentiality of information systems" in a case involving the lawfulness of an amendment to the Act on the Protection of the Constitution in North Rhine-Westphalia concerning new investigative techniques to intercept communications via the Internet (Schafer & Abel, 2010). The constitutional complaint was filed by four plaintiffs,[16] including one lawyer assisting asylum-seekers and a journalist who visited websites and chats to investigate extremist cells in the country. Second, in 2022, the BVerfG ruled, in the BvR 2354/13 case also filed by an individual citizen monitored by the BfV, that the sharing of personal data gathered by the agency via covert methods (such as device hacking) with state police authorities and public prosecutors without observing the safeguards to fundamental rights was unconstitutional. The Court held that this practice affects the right to personality "in its manifestation as the fundamental right to informational self-determination"[17] and violates the principles of legality, proportionality, and necessity, a ruling that gives rise to the principle of separation of police and intelligence data (Bundesverfassungsgericht, 2022).[18] Third, in 2020, the ruling in the BvR 2835/17 case, filed by CSOs Reporters Without Borders and Gesellschaft für Freiheitsrechte, stated that foreign surveillance oversight was below minimum standards, resulting in the creation of the UKR (Bundesverfassungsgericht, 2022; Kniep et al., 2023).

The possibility for a citizen or an organization to file a constitutional complaint before the BVerfG must be considered a critical aspect of democratic oversight, increasing social recognition and representation in judicial paths that will shape the public debate over public interest matters.[19] All the aforementioned decisions were filed by individuals or CSOs before the BVerfG and have triggered reforms to the legal framework concerning limitations to the use of hacking techniques. These cases thus illustrate democratic ways of meaningfully accessing justice.

---

16 To have the legitimacy to do so, the individual or organization has to prove that they are directly affected by an act of the state and that a fundamental right secured by the German Constitution is violated – an extraordinary remedy established by its Article 93(1) n. 4a and b. See further legal prerequisites in Bundesverfassungsgericht (2024).

17 For a comprehensive view of the right to informational self-determination, see Albers (2005) and Schertel (2020).

18 See footnote n. 8.

19 For an overview of the state of civil society freedom in Germany, see Hummel, Pfirter, and Strachwitz (2022).

From a historical perspective, as stated by Miller (2016), government intelligence services in Germany are a sensitive topic and have generated more substantial resistance than in other countries, mostly because of the totalitarian past and resulting post-war sentiments. Authors even mention some level of historical aversion to United States surveillance among German nationals, fueled by the Snowden revelations. The BND was created and operated within the NATO framework and with direct American operational control during the Cold War, "giving Americans a unique intelligence asset inside the West German government" (Krieger, 2010, p. 1). The famous 1983 BVerfG's census ruling that triggered the recognition of the right to information self-determination (Albers, 2005; Schertel, 2020) can be seen as a historical piece of such a collective affection. Citizens have assimilated the notion that privacy and sovereignty are public goods that cannot be taken for granted and that independent arbiters are necessarily required (Wetzling, 2023b). As a result, contemporary BVerfG rulings and institutional improvements to intelligence oversight come on the heels of numerous public concerns (at the state and citizen levels) about the processing of personal data and should be understood through a historical lens.

3.2 The Case of Brazil

The intelligence ecosystem in Brazil encompasses the Brazilian System of Intelligence (*Sistema Brasileiro de Inteligência*, Sisbin), which has the federal Abin at its center. Abin has effectively been active since 1995, although it was officially created with the enactment of the Law 9883/1999 (Brandão, 2002). The law also established Sisbin and its sub-units in each Brazilian state – without, however, specifying how these bodies would be integrated or the nature of their relationship with Abin (Carpentieri, 2017). Currently, Sisbin comprises 48 units spread throughout the country. Both the system and the agency were under the Cabinet of Institutional Security, historically chaired by military representatives, until 2023 when Abin was transferred to the Civil Office (*Casa Civil*), a body that directly assists the presidency in carrying out its functions related to the administration of other bodies at the federal level and provides advice on political and institutional relations (Casa Civil, 2023). Abin carries out both domestic and foreign intelligence activities.

In 2013, 14 years after the institutionalization of Abin, which followed the formal transition to a civilian government in the 1990s, an oversight body was created in the Brazilian Congress: the Joint Commission for the Control of Intelligence Activities (*Comissão Mista de Controle das Atividades de Inteligência*, CCAI) (Bruneau, 2015). The sole specialized external oversight body, the CCAI is composed of 12 members of the parliamentary branch, including the presidents of the Commission on Foreign Relations and National Security (both from the Senate and Federal Chamber of Deputies), leaders of the "minority" and "majority" in parliament (both from the Senate and Federal

Chamber of Deputies), and three members of each parliamentary branch, with a 2-years mandate (Câmara dos Deputados, 2013). [20] It has the administrative mandate to oversee intelligence activities. Therefore, Brazil has so far implemented a centralized model of external oversight.

Sisbin replaced the National Service of Intelligence (*Serviço Nacional de Informação*, SNI), the intelligence apparatus of the Brazilian dictatorship, within the scope of the "negotiated redemocratization" (Brandão, 2002; Cunha, 2010).[21] Consequently, some public services were not subjected to major constitutional revision. According to intelligence scholars in the country, while the contemporary intelligence apparatus supplanted the SNI and despite the change in terminology from "information" to "intelligence," it inherited a rationale that constructs an intelligence system far from effective accountability and transparency requirements (Brandão, 2002; Capentieri, 2017; Zaverucha, 2008; 2010). Due to its long-negotiated transition to a democratic regime, the current Brazilian Constitution of 1988 tellingly does not even mention intelligence activities and their basic principles or purpose. This is because security and defense reforms were strongly resisted by the remaining military power.

Over the last few years, Abin has faced numerous scandals involving the monitoring and profiling of political figures, especially during the administration of former president Jair Bolsonaro. To name but a few, in 2020 it was revealed that the Secretary of Integrated Operations (*Secretaria de Operações Integradas*, Seopi), an intelligence sector under the Ministry of Justice and Public Security and part of Sisbin responsible for integrating the actions of public security entities from the states, especially in organized crime cases, was producing dossiers profiling public employees involved in antifascist movements in Brazil, including professors. Abin was among the public bodies the dossiers were sent to (Teixeira, 2020). The case was followed by an STF ruling prohibiting such activities: according to Justice Carmen Lúcia's opinion, "intelligence activities must respect the democratic regime, in which the persecution of opponents and the political apparatus of the State are not permitted," and "the history of abuses reported regarding the intelligence service highlights the imperative of effective control of such activity" (Supremo Tribunal Federal, 2022). In 2021, the Supreme Court also ruled on limits to data sharing between Abin and the other bodies that constitute Sisbin, stating that requests for sharing personal data must respect the public interest, the defense of public institutions, and have a proven purpose (Supremo Tribunal Federal, 2021). The ruling tackled a Presidential Decree by then-President Bolsonaro establishing that a simple request by Abin would be sufficient for the agency to

[20] For more detailed information, see Câmara dos Deputados (2013): "Resolution n. 2/2013-CN: Provides for the Joint Commission for the Control of Intelligence Activities (CCAI), a permanent commission of the National Congress, an external control and oversight body for intelligence activities, provided for in Art. 6 of Law No. 9,883, of December 7, 1999" (my translation).

[21] As revealed in a study by Ishaq and Franco (2008) on the Brazilian National Archive, more than 300,000 citizens were profiled by the SNI during the Brazilian dictatorship, many of whom were tortured and murdered by public authorities. The transition of the SNI to Abin was part of the process of "reconciliation" between civilians and military forces.

receive data from all Sisbin bodies, which was later understood as unconstitutional by the court (Supremo Tribunal Federal, 2020a).[22] Moreover, in 2022, it was revealed that Abin had been using the software FirstMile,[23] developed by Israeli-based company Cognyte, to monitor thousands of telephone numbers and their live locations, including those of members of parliament, activists, and journalists, without a warrant issued by any regular court (Dantas & Bronzatto, 2024).[24]

The Abin-Gognyte political case above was followed by a Claim of Non-Compliance with a Fundamental Precept (ADPF 1143) before the STF, filed by the General Prosecutor's Office (Procuradoria Geral da República, PGR) at the beginning of 2024 (Supremo Tribunal Federal, 2023a). The PGR argues that there is a regulatory omission in the use of "remote virtual intrusion programs and secret and invasive monitoring tools for personal digital communication devices." Accordingly, it seeks the legislative obligation of the Federal Congress to regulate the issue: "the mere existence of hacking programs can have chilling effects on freedom of expression, on the work of the media and on public debate and participation, potentially undermining democratic governance," citing a report by the UN High Commissioner for Human Rights (Ramiro, 2024). The lawsuit also asks for the Court to establish norms for these procedures while Congress does not address them.[25] Although the lawsuit is pertinent in that it pushes the STF to develop a legal understanding of the phenomenon according to the fundamental rights in the Brazilian Constitution, it may fall short of framing the legality of hacking operations, notably because the country does not have data protection regulation for intelligence or law enforcement activities, areas that are outside the scope of the 2018 National Data Protection Law.[26] In addition, the activities of intelligence agencies are still weakly regulated, and their oversight is below basic standards. In sum, the lack of a systematic understanding of hacking activities in terms of their hypothetical uses, proportionality, and necessity principles according to data protection parameters, as well as the lack of checks and balances with fundamental rights, should be dealt with before regulating government hacking.

---

22 Some political analyses connect the decree to Bolsonaro's aim to obtain secret information from the Federal Police about corruption investigations against his sons (Richter, 2024; Peron et al., 2024).

23 The service works by exploiting a vulnerability in the SS7 protocol used in telecommunications systems.

24 At the time of writing, the surveillance program has already resulted in the arrest of two Abin employees and the removal of many of its directors.

25 A further critique of the constitutional lawsuit was made by an amicus brief by the Brazilian Institute of Criminal Sciences, arguing that the action should not be recognized because "the inclusion of a new rule in the constitutional text [the right to the protection of personal data], through the action of the derived constituent power, suggests significant changes in social values or in the empirical framework underlying them. It implies that constitutional rules and regulations in force until then are not sufficient to provide an adequate response to social changes… If the present ADPF proposed to point out the unconstitutionality of the use of government hacking technologies, its admissibility would be indisputable. But no, the intention is for the Supreme Federal Court to produce a rule restricting rights provided for in fundamental precepts, which, it should be noted, operate fully in the absence of regulation" (Arguição de Descumprimento de Preceito Fundamental n. 1143, 2024) (my translation).

26 Even though Art. 4, §1, states that further legislation on the matter must strictly respect the principles of proportionality and necessity according to the public interest of data processing in these sectors, due process, and the set of general principles of the National Data Protection Law.

Meanwhile, as concerns Abin's external oversight, the CCAI lacks the necessary enforcement capabilities and expertise; as a result, there are no meaningful external oversight mechanisms for intelligence activities in Brazil (Cepik, 2021; Bruneau, 2015; Carpentieri, 2017; Gonçalves, 2010). Sisbin's recent surveillance episodes were not even examined by the commission, including the "Excel Project" – a Seopi program that encompassed the provision of Cellebrite's mass data extraction tools to state law enforcement authorities in exchange for data about criminal investigations (Ameno, 2022), or the use of Córtex (Rebello, 2020), an artificial intelligence tool for gathering and cross-analyzing data from several databases, from live CCTV to automatic cameras that read cars' license plates, as well as the addresses, salaries, and daily routes of citizens.[27] Thus, the CCAI lacks transparency, does not maintain proper patterns of scrutiny of intelligence activities, and publishes minimal information regarding its activities in response to complaints by other parliamentarians and civil society.

Therefore, the "idleness" of the CCAI points to a systemic external oversight problem in Brazil. In 2017, the Commission met only twice and merely to discuss its budgetary implementation (Valente, 2023); between 2018 and 2020, it met once. Parliamentary control of such activities is subject to political influences and interferences from political parties (Cepik, 2021), as evidenced by exchanges of positions on the Commission to ease governmentality, which is part of a culture in the Brazilian political institutional ecosystem.[28] The CCAI is solely composed of parliamentarians, who often lack expertise about security and intelligence accountability – a problem that also affects other oversight institutions, such as judicial bodies that rule on requests for surveillance measures. The expertise is fundamental and separates countries like Brazil from others that have quasi-judicial bodies in charge of the *ex-ante* oversight of surveillance activities, such as the G10 Commission and the UKR in Germany or the Foreign Intelligence Surveillance Court in the United States, although these bodies are not without problems.[29]

---

27 In this regard, an interesting survey by the CSO Data Privacy Brasil showed that the CCAI has been silent about many surveillance episodes reported by members of the Brazilian Parliament, the press, and CSOs (Vergili, 2022).

28 For instance, congressman Alexandre Ramagem, who chaired Abin at a time when several illegal surveillance activities were carried out and is under investigation by the Federal Police, is currently a member of the CCAI.

29 The participation of the Public Prosecutor's Office as – theoretically – a counterbalance or "necessary adversary" to the suspension of fundamental rights such as privacy and the secrecy of communications, is a good oversight and procedural practice. Concerning the United States, which does not rely on such counterbalance, Sharon Bradford Franklin recalls the argument of former US judge James Robertson that "judges are learned in the law and all that, but anybody who has been a judge will tell you that a judge needs to hear both sides of a case before deciding." This is also what the US Privacy and Civil Liberties Oversight Board recommends (Franklin, 2020).

Parliamentary oversight is intrinsically marked by both potentialities and weaknesses. As noted by Zegart (2000, 2011), congressional external oversight could be seen as the most democratic tool for monitoring intelligence agencies because it is – *on paper* – the direct representation of the people, unlike data protection commissioners and members of judicial bodies, for example. Yet, beyond the lack of expertise, it comes with specific deficiencies, such as the internal influence of politics and a tendency to avoid bureaucratic or *transaction costs* when intelligence information is protected by secrecy regimes. To lift the curtains of intelligence information, even when legally mandatory, spending political capital is required, which parliamentarians and even voters and campaigners are often insufficiently interested. Quoting a staff member of the American Congress, "legislators can't go home and hold intelligence awareness fundraisers in the district" (Zegart, 2022, p. 279). This also applies to the Latin American landscape, where socioeconomic policies historically speak louder than security agendas because of economic inequalities (Olliveira, 2023; Zaffaroni, 2007).

The Brazilian scenario points to an even further challenge concerning access to information by the parliamentary oversight body, especially when the bulk of exploitation technologies used by the intelligence sector is offered by international private vendors (Ramiro et al., 2022). Conducted as a lawful business deal, the acquisition, hiring, and training process for the use of these tools comes from an international and unregulated gray market of vulnerabilities trade (Fidler, 2015), which poses challenges to administrative law regarding rules of government procurement (Anstis, 2021). The public-private assemblage of surveillance systems, together with a toothless institutional design and domestic politics, creates an opaque accountability regime of intelligence services that lowers the bar of democratic oversight.

4 Highlighting Democratic Oversight Aspects and Opportunities for Improvement

Drawing on the central elements of democracy according to Habermas (1992), especially in his co-originality thesis, we must remember that official and civic participation, in its pluralism, are fundamentally connected in designing an institutional arrangement and openness for public participation. This entails assessing the effectiveness of institutions, their fundamental flaws and potentials, their participation level, and their track record in balancing different stakeholders' agendas. It also means analyzing the state of civil society engagement such as litigation before courts, the freedom of the press, and meaningful access to information about government activities. Narrowing this scope, Roller et al. (2023) develop the notions of *delegated* oversight, namely, "external bodies bestowed with legal oversight mandates," and *civic* oversight, that is, "practices

by the media, CSOs, and citizens who complement delegated oversight through an oftentimes more adversarial and more public mode of oversight" (Wetzling, 2023a, p. 248 – 249). These aspects serve as an initial "toolkit" for assessing the democratic level of intelligence oversight in both countries.

In the case of Germany, the first interesting policy development is semantic, specifically the establishment of an independent taxonomy for techniques made possible by the exploitation of vulnerabilities (*Quellen TKÜ* and *Online Surchsuchung*, for instance), grounded in BVerfG decisions and federal laws, each followed by procedure, limitations, and the provision of an oversight model. However, current debates over the extent of these techniques, the lack of a "Vulnerabilities Equities Process-like" policy (Herpig, 2018; Franklin & Thompson, 2017), and initial international cooperation over the control of spyware markets such as the Pall Mall Process (Foreign, Commonwealth & Development Office, 2024) are yet to be further discussed internationally towards the creation and harmonization of such assessments.

Institutionally, a network of oversight bodies is taking form, with possible overlap between their tasks (Bundesbeauftragter für den Datenschutz und Informationsfreiheit, 2020).[30] The Parliamentary Oversight Panel and the CCAI, for instance, are important assets because each institution is composed of democratically elected representatives, and, as stated by Wills and Vermeulen (2011), society mandates parliaments to hold security agencies accountable in the fulfillment of their powers, which includes approving the allocation of public budget to fund security agendas. However, this model does not fulfill expertise requirements or avoid the political interplay within parliaments, whose members constantly calculate the political capital they spend on holding intelligence agencies accountable (Zegart, 2000, 2011). Ways for improving parliamentary oversight, especially in the case of government hacking activities, could and should consist in enforcing a "chain" of oversight entities: the judiciary branch is not the only entity that can decide on the necessity of legislative reforms; CSOs must also play a central role in pushing for the integrity and effectiveness of such legislative control, be it by institutional means or via the press, public awareness campaigns, litigation, and advocacy efforts (Kniep et al., 2023). The set of parliamentary oversight improvements can also be enriched with mandatory resources that improve transparency mechanisms, such as enforcing the frequency of public reports, strengthening prerogatives for its parliamentary members to initiate investigations, and emphasizing dissenting opinions.

---

[30] According the 2020 Activity Report of the BfDI, "although a completely independent supreme data protection supervisory authority exists in Germany with my authority, which has a high level of expertise and many years of experience in data protection and thus intelligence service control of the BND and the domestic intelligence services of the Federal Government, the Federal Government intends to create a new supreme federal authority, the 'Independent Control Council'" (Bundesbeauftragter für den Datenschutz und Informationsfreiheit, 2020). However, while safeguarding the effectiveness of intelligence services, being too cautious may be better than allowing possible loopholes or the lack of a legal mandate for competent authorities to oversee intelligence agencies.

Specialized non-parliamentary oversight bodies provide the expertise that legislative committees often lack. They are mostly composed of members who possess particular judicial and/or technical qualifications and are not deeply enmeshed in the power plays of parliaments. In the case of Germany, the UKR and the BfDI, for instance, are not directly elected by the people but contribute to the oversight system with mandates and expertise in risk assessments relative to fundamental rights and security parameters and requirements in cases involving SIGINT surveillance, such as the use of hacking tools. Notably, the role of the BfDI is central to addressing concerns from a contemporary data protection standpoint. The BfDI has an independent mandate to review permissions issued by the G10 Commission; it also publishes annual "activity reports" detailing the audits performed by the Commissioner, including in the intelligence sector. Furthermore, it offers institutional channels for CSOs to lodge complaints about the processing of personal data, including in the realm of intelligence activities (for example, when surveillance powers are outsourced to the private sector).[31] However, an institutionalized multistakeholder council integrated into the BfDI is missing from the architecture of data protection governance in the country. The complex nature of data protection regimes (Albers, 2015) and their authorities require both a high level of expertise and the composition of bodies through democratic elections. Therefore, a good governance practice is the establishment of institutionalized channels for public participation, such as a multi-stakeholder council like the Brazilian National Board of Data Protection and Privacy,[32] which can provide input and help the data protection authority to shape its agenda, taking into account public, private, technical, and social concerns (Raymond & DeNardis, 2015; Gasser et al., 2015).

A progressive due process in the realm of intelligence activities is exemplified by the institutionalization of instances specialized in ex-ante assessments of the legality of surveillance requests, including those based on the use of hacking tools, such as the G10 Commission and the UKR. Theoretically, the fact that these bodies conduct specialized oversight control differently from regular courts of justice, which often lack expertise in cybersecurity technical safeguards, is a judicial advance. Nonetheless, as noted by Wetzling (2023b), the members of these bodies do not have to listen to the arguments of the people

---

[31] The Gesellschaft für Freiheitsrechte (GFF) did this a number of times, pushing the BfDI to scrutinize the matter. See, for example, Gesellschaft für Freiheitsrechte (2021a). CSOs have also scrutinized systems and made technical contributions to audit activities. This was the case of the Chaos Computer Club (2019), which audited a spyware from the then German-based company FinFisher.

[32] Its attributions are to "propose strategic guidelines and provide support for the development of the National Policy for the Protection of Personal Data and Privacy and for the actions of the ANPD; Prepare annual reports assessing the implementation of the actions of the National Policy for the Protection of Personal Data and Privacy; Suggest actions to be carried out by the ANPD; Prepare studies and hold debates and public hearings on the protection of personal data and privacy, and; Disseminate knowledge about the protection of personal data and privacy to the population" (my translation).

affected (or their representation) in the decision-making process, which raises concerns when it comes to safeguarding the human right to a fair trial.[33]

The case of Brazil illustrates quite the opposite situation, as mentioned above. In law enforcement cases, the government bodies responsible for assessing the legality of surveillance requests are regular courts of justice, but the examination of requests for surveillance measures (from wiretapping to hacking operations) must normally take into account the opinion of the Public Prosecutor's Office as a legitimate institutional protector of collective rights, that is, as *custos legis* or the "guardian of the legal order." Although the *custos legis* nature of the Public Prosecutor's Office is debatable in the criminal procedure doctrine – some argue that it cannot be the *prosecutor* and an *oversight* institution at the same time – its role represents a democratic advancement in the Brazilian Constitution, and the doctrine on the topic is vast (Supremo Tribunal Federal, 2023b; Mazzilli, 2022; Arantes, 1999). Beyond proposing actual prosecutions in the context of investigations, the Public Prosecutor's Office must normally be notified when a warrant (e.g., for telecommunication surveillance, acoustic signals in public spaces, or evidence from an illegal source) is requested and issued, ensuring the proportionality of the measure, and, as a result, enforcing checks and balances regarding fundamental rights if it deems the request to be beyond the legal parameters. The Office is also responsible for initiating civic public inquiries to investigate whether a collective right has been violated and for applying monetary penalties, whose proceeds go to the Fund for Defense of Collective Rights (*Fundo de Defesa dos Direitos Difusos*). This Fund aims to redress the harms caused to the collectivity, as can be the case of government hacking abuses.

Furthermore, Brazilian intelligence activities by Abin, for instance, don't count on constitutional provision - defining its mission and scope - and its surveillance measures do not go through a regular due process (for instance via special courts with mante to assess their legality), assessing its legality. This is a central loophole in terms of intelligence control and, as a result, accountability to its central intelligence agency. It is safe to assume that the majority of the public only has access to its activities via whistleblowers and press exclusive coverage. And, as mentioned, although "further regulation" in the area has to respond to proportionality and necessity principles according to the Brazilian Data Protection Law, the current regulation leaves outside its scope the oversight of intelligence activities. It means that the National Data Protection Authority does not have a mandate to oversee intelligence operations. Such reforms are fundamentally necessary to the creation of a decentralized model of oversight and has to take a structural approach of institutions and means of civic participation.

---

[33] According to Wetzling (2023b), "Germany has not yet opted for a direct representation of the interests of affected groups in the authorization process. Instead, the members of the G10 Commission solely hear the arguments of the German government prior to their decision-making on the admissibility and necessity of individual or groups of cases. (p. 7).

Finally, the role of the National Council of Justice (*Conselho Nacional de Justiça*, or CNJ) is central to the Brazilian oversight system of the judiciary and must be further discussed. The CNJ is responsible for administrative and financial control, as well as overseeing functional duties of the judiciary branch, including planning and executing policies to improve the role of the courts of justice. The CNJ must do more to implement its legal mandate (as it does with regular telecommunication surveillance measures through the "National Telephone Interception Control System") (Conselho Nacional de Justiça, 2024) by also monitoring warrants for exploitation surveillance and reporting regularly on the number of requests and how many were implemented. This improvement is crucial to understanding the extent and efficiency of these techniques in quantitative terms.

Another central element shaping the public debate around government hacking activities and oversight of intelligence agencies is the set of extraordinary legal remedies for controlling constitutionality, especially civil society entities' standing to access justice before the supreme courts. Although relatively comprehensive, the set of civil entities in Brazil with standing to pursue such actions[34] comprises the Federal Council of the Bar Association, political parties with representation in the Brazilian Congress, confederated trade unions, and "class entities" working at the federal level with representation in at least nine Brazilian states and a direct connection between the subject of their request and their statutory objectives (Sarlet et al., 2020). As noted by Gomes (2010, p. 159), whereas Germany provides universal standing for any citizen, national or foreigner, to exceptionally lodge a constitutional complaint before the BVerfG if any of their constitutional rights are violated, in Brazil, "broad popular participation in the control of constitutionality… making possible the formation of an open society of interpreters of the Constitution" has been vetoed based on the argument that it would make the work of the STF impossible (Presidência da República, 1999).[35] This is a fundamental difference between these two constitutional law systems, which is reflected in the democratic oversight of government activities, including surveillance by intelligence agencies.

---

[34] Importantly, this depends on the claim and the chosen extraordinary remedy, each of which has its own regime of standing. Here, we consider the Claim of Non-Compliance with a Fundamental Precept and the Direct Action of Unconstitutionality. Beyond those listed, the President of the Republic, the Board of the Federal Senate and of the Chamber of Deputies, the Board of the Legislative Assembly or the Legislative Chamber of the Federal District, the Governor of the State or of the Federal District, and the General Prosecutor's Office also have a standing to pursue such actions.

[35] According to the justification of the veto (Presidência da República, 1999), "it is unnecessary and inefficient to admit the excess of cases to be processed and judged, certainly resulting from unrestricted and individual access to the Federal Supreme Court. As the facts to be examined multiply without ensuring their relevance and social transcendence, the additional compromise of the functional capacity of the Federal Supreme Court constitutes an unequivocal offense to the public interest" (my translation). This is a valid argument, and recent data about the overwhelming amount of judicial processes support this statement (Conselho Nacional de Justiça, 2022). Nevertheless, the narrower set of institutionalized parties legitimated to control constitutionality – in the sense of bringing cases directly to the STF, bypassing previous instances – works as gatekeepers to the interpretation of the Constitution, which often entails transactions of considerable political capital. In light of political *representation* claims, as noted by Fraser (2008), "often procedural disagreements translate into disputes over representation or political voice. Where one party would restrict representation in dispute-resolution bodies to states, others countenance representation for NGOs, and still others envision cosmopolitan democratic schemes that directly represent individuals *qua* world citizens" (p. 399).

The constitutional regime concerning access to justice is among the primary sources for setting public policy agendas, and doing so contributes to building legal bases for the regulation of intelligence activities as a result of legitimate demands raised by civil society. In the case of Germany, *constitutional complaints* lodged before the BVerfG by CSOs such as Netzpolitik, Reporters Without Borders, and Gesellschaft für Freiheitsrechte have shaped the constitutional framing of government hacking routines and have catalyzed modifications to legislations such as the Code of Criminal Procedure, the G10 Act, and the laws that regulate the work of the BND Act and BfV. This direct access to the BVerfG through means of "control of constitutionality" constitutes the mosaic of democratic intelligence oversight in its *civic* dimension, which affects the institutional design of the government by improving and creating new accountability requirements. For reference, as of 2020, close to 5,200 constitutional complaints had been filed, accounting for 94% of the judicial remedies filed before the BVerfG (Bundesverfassungsgericht, 2020).

However, the high number of constitutional complaints dismissed on the basis of a lack of standing of the plaintiffs related to the object of contestation or because the plaintiffs do not comply with due judicial proceedings (e.g., not seeking prior judicial remedies before lower courts; i.e., the principle of subsidiarity) must be noted. In the realm of secret surveillance contestation, for instance, this was the case of a constitutional complaint lodged by the Gesellschaft für Freiheitsrechte and Computer Chaos Club Stuttgart against the Baden-Württemberg Police Act, which questioned the legality of exploiting vulnerabilities without a prior consolidated assessment of whether public authorities should leave vulnerabilities unreported and unpatched (Bundesverfassungsgericht, 2021). Although the BVerfG dismissed the complaint precisely because of the principle of subsidiarity, the Court confirmed that "state authorities violate fundamental rights when they keep security gaps in IT systems secret without assessing their risks," which was considered a success by the plaintiffs (Gesellschaft für Freiheitsrechte, 2021b). In parallel to the problematization of the standing standard for filing judicial remedies before the BVerfG, the success of strategic litigation can be measured by more complex metrics beyond the full acceptance of plaintiffs' claims.

Meanwhile, in Brazil, although CSOs must rely on another standing regime of control of constitutionality, they have also accessed judicial bodies to question the legality of intelligence agencies' activities, including in cases involving surveillance technologies. This was the case of a request by non-governmental organizations (NGOs) such as Instituto Igarapé, Conectas, Sou da Paz, and Transparência Internacional Brasil before the Federal Court of Audit (*Tribunal de Contas da União*) demanding that a public bid of the Ministry of Justice and Public Security, which initially had the spyware maker NSO Group as a competitor (Conectas Direitos Humanos, 2021), be blocked, leading the company to drop out of the competition. More recently, the NGO Data Privacy Brasil (2023) requested the Federal Public Prosecutor's Office (*Ministério Pú-*

*blico Federa*l) to investigate the use of Cognyte's geomonitoring tool (First-Mile) by Abin. Finally, civil society entities also actively participated in a few cases before the STF concerning restrictions to state surveillance capabilities involving end-to-end encrypted communications with *amicus* briefs, helping to shape the rationale for the STF's decisions in such cases (Supremo Tribunal Federal, 2020b). Nonetheless, as mentioned above, the gateway for NGOs to pursue constitutional remedies is considerably narrower than in Germany. Even so, the available venues for accessing justice have been central to CSOs demanding action from *official* oversight authorities and participating in strategic lawsuits to question intelligence surveillance activities overall.

Considering that claims for transparency and accountability for private providers tend to have lower force than those for public bodies and that most services in the realm of hacking technologies are offered by private contractors, several authors (Anstis, 2021; McKune, 2019; McKune & Deibert, 2017) have pointed out avenues for improving intelligence accountability by anchoring it in contractual clauses grounded in public values in government procurements. Drawing on Anstis (2021), measures for improving government hacking oversight may include *a*) a centralized "cyber institution"[36] with proper expertise and strategic coordination, integrating different government entities responsible for managing such contracts both *pre* and *post* sale, and accounting fully for the diversity of the government's defensive and offensive cyber capabilities, together with an external public ombudsperson with a mandate to oversee the use of government hacking tools; *b*) proof of the company's compliance with privacy and data protection laws in the domestic jurisdiction, combined with regular audits by domestic authorities;[37] and *c*) an international human rights reputational assessment to narrow the risk of governments financially contributing to companies that also contract with authoritarian states, harass civil society actors, and are associated with cyberwarfare and cyberattacks, with an eventual blacklist of specific vendors.[38] These measures are to be considered within the legal framework of both countries, taking into account their rules concerning public contracting and their intelligence oversight mechanisms, in particular their courts of audit, trade control rules, and cybersecurity authorities.

---

[36] On the German side, the creation of the Central Authority for Information Technology in the Security Sector (*Stelle für Informationstechnik im Sicherheitsbereich*, or ZITiS) is the most recent effort to build a central "cyber institution" to mediate contracts with spyware vendors. It faces several critiques, however (Meister, 2018, 2023). On the Brazilian side, the military is pushing to create the so-called National Agency of Cybersecurity (*Agência Nacional de Segurança Cibernética*, or ANCiber). See also the critiques in Motoryn (2024) about the military composition of the proposed agency.

[37] In its 2019 Report, the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye (2019, p. 18), also suggested that to comply with international human rights standards, companies must adopt contractual clauses "that establish clear and specific prohibitions on product customization, targeting, servicing or assistance that violates international human rights law."

[38] At the time of writing, neither the member states of the EU (including Germany) nor Brazil have so far adopted blacklisting measures like the United States under the Biden administration. See Lubin (2023). Furthermore, an example of governments defunding spyware companies is provided by Norway, which excluded the hacking company Cognyte from its investment fund (Council on Ethics, 2022).

Domestic efforts to ensure the democratic oversight of intelligence services can also take advantage of multilateral cooperation aiming to address the arbitrariness and proliferation of exploitation technologies. Engaging in such efforts will have international implications for domestic misuses and push for clearer and more solidified national regulations. Examples are the PEGA Committee (European Parliament, 2023) – a public inquiry body that brings together several parliamentary and executive government authorities of European member states and produced a thorough report including policy recommendations – as well as the Pall Mall Process – an international agreement signed by nearly 30 countries, which seeks to curb the adoption of commercial spyware by governments. Another example is the further enforcement and update of the Wassenaar Arrangement, which provides guidelines for export control of dual-use technologies within domestic legislation to hold accountable countries that export exploitation technologies without prior state permission (Zvi, 2023).

Although soft-law instruments, these tools can be explored by the international community, including Brazil and Germany, to harmonize mechanisms of democratic oversight of intelligence services, especially as concerns the use of hacking technologies. More jurisdiction-oriented regional efforts, including necessary amendments to surveillance and human rights regulations, might also strengthen the role of regional courts, such as the Inter-American Court of Human Rights and the European Court of Justice, in establishing new paradigms of fundamental rights that will counterbalance and constrain domestic surveillance. Finally, borrowing from Anstis's (2023) analysis of international espionage of political dissidents, the "inclusion of the requirement to cooperate internationally on this issue and creation of a forum for such exchanges to happen on a regular basis would be likely to lead to more streamlined and consistent information-sharing" (p. 273). A multi-layered focus on improving human rights standards should therefore be fostered at the diplomatic and multilateral policy levels to enforce domestic legal frameworks.

Finally, the logic of creating a vulnerabilities equities process (VEP) for assessing whether to disclose a vulnerability to the developer of an application, network, or hardware (such as Google, Meta, Microsoft, or Apple) for patching or use it for intelligence or law enforcement purposes is a possible avenue for broadening the oversight system in the administrative process of developing or procuring technologies that rely on *zero-day* vulnerabilities[39] (Herpig & Schwartz, 2019; Herpig, 2018; Franklin & Thompson, 2017). Regarding the latter, a decision-making process by public authorities could intervene before contracting with a private company to assess the risks associated with acquiring such technology. In addition, *ex-post* evaluations of the contract could confirm or lead to a reinterpretation of a previous VEP model, with the public authority potentially terminating the contract. Representativity within the

[39] A vulnerability in a technology system unknown to its developer, who therefore has "zero days" to patch it before the vulnerability is exploited.

VEP could rely on trusted third parties from academia and civil society, such as cybersecurity and consumer protection organizations (Thompson, 2021) to make the process more democratic. This would entail formulating government agendas thoroughly by addressing the political, social, and technical concerns raised by different stakeholders.

Another initiative worth discussing is the possibility of an International Vulnerabilities Equities Process (VEIP) in the realm of cyber-norms, with the creation of an International Vulnerability Review Board. Schulze (2020) considers that, although the contemporary lack of reliability of the attribution of cyberattacks and weak enforcement of sanctions for non-compliant state behavior makes its establishment fragile, a VEIP model could at least assess the use of zero-days vulnerabilities (instead of including other types of vulnerabilities) in cyber operations given that several countries recognize the high risk posed by their instrumentalization. This model could facilitate the inclusion and participation of the technology industry in setting up procedures, taking advantage of existing systems of vulnerability disclosure (e.g., competition between bug bounty programs) (Fidler, 2015), and help to mediate power asymmetries in states' cyber-capabilities.

Therefore, beyond the mutual influence between the models of oversight of Brazil and Germany, their participation in the international realm may build on multilateral discussions and actual policy-making processes that would encourage the development of domestic regulatory models of intelligence agencies and hacking practices. Bringing together local and global perspectives on the regulation of these tools and government agencies may help to create checks and balances at the national and international levels given the cross-border potential of cyber operations such as government hacking.

5 Conclusion

The issue of democratic oversight of government hacking by intelligence agencies is in a flux given its current policy development and sociotechnical understandings. While comprehensive regulations on the domestic and international levels are lacking, significant progress and political engagement by public authorities and CSOs have helped shape the public debate around intelligence activities and the use of hacking technologies, often in reaction to public scandals. Establishing a proper semantic framework for this subject, based on either technological concepts or intelligence-investigatory routines, is fundamental to academic discussion and policymaking processes. At the same time, it is natural to *continuously re-discuss* how new techniques fall into these categories and eventually create novel paradigms based on new sociotechnical realities and assessments of their legality, proportionality, and necessity. Developments in

surveillance tools must be continuously assessed before their actual implementation based on their risks and impacts on the ecosystem of rights.

As the public interest in intelligence activities is far from a political priority, especially in countries with pronounced socioeconomic asymmetries (e.g., Brazil), fostering avenues for civil society participation as a democratic oversight asset is all the more important. Efforts to push public authorities to act, such as judicial courts, have been at the epicenter of transformative changes in domestic legal frameworks. Therefore, strengthening *civic* oversight of intelligence services and its enforcement by *official* authorities is crucial to harmonizing the protection of human rights while assessing the political and social implications of these operations. This does not mean that all technologies that aim to exploit vulnerabilities are to be legitimized[40] but rather that a trustworthy and democratically built due process must be in place, which includes the possibility of prohibiting the development or procurement of some technologies through reliable administrative and judicial processes.

Additionally, there is no single model or single government body capable of performing "perfect" oversight, covering representativeness, legitimacy, and expertise in intelligence and government hacking activities. Instead, an oversight governance system comprised of multiple authorities with different tasks, together with democratic venues for public participation, must be tailored to domestic legal frameworks and institutions. Second, domestic legislation regarding intelligence and hacking activities must be in dialogue with international collaborations and agreements, necessarily including multilateral organisms. This should also be further explored by international law research. The development of hacking tools is not only inscribed in domestic intelligence agendas but also intrinsically part of states' strategies active in cyberwarfare and of a global private industry. This makes it even more difficult to draw lines between its use for national security purposes and for domestic public security, especially when it comes to international cooperation and foreign intelligence activities.

Taking Germany and Brazil as case studies as one of many possible legal comparisons helps nuance our understanding of the phenomenon. As discussed in this paper, the institutional and political history of each country shapes the *status quo* of the problem and results in the necessity for an harmonized understanding by different stakeholders to identify avenues for democratic improvement and legitimate public participation. This is a task for multiple stakeholders involved in the governance of such activities and highlights not only the dynamism of jurisdictional analysis but also how the exploitation of

[40] Neither do *all* intelligence activities. Bigo et al. (2024) recall that the US-based historical doctrine of intelligence studies has produced "theories for and not of intelligence" and argue that "an imaginary of a world in which state affairs – and in particular foreign affairs – are exempt from democratic rules and are left to opportunistic decisions is left intact, complete with all its misconceptions and fallacies. Such a framing typically downplays the violence carried out by secretive agencies and normalises the right for government authorities to surpass democracy and the rule of law if they deem it necessary" (p. 1).

vulnerabilities has been – and continues to be – a concern for different sectors. As concerns judicial systems and control of constitutionality in each jurisdiction, further developments on the topic could also improve the comprehension of the differences and complexities of plaintiffs' standing status in pursuing judicial remedies before national constitutional courts and regional courts when dealing with regional treaties, especially in connection to the field of state surveillance and civic participation that reinforce the democratic nature of these activities through channels of effective oversight.

The architecture of the democratic oversight of intelligence agencies is a central topic in surveillance, intelligence, and security studies due to the new challenges created by the growing adoption of hacking technologies, which is a relatively new field of investigation. Therefore, policy continuity and academic developments are required to offer open and effective mechanisms for involving affected stakeholders as a possible barometer of democracy and social justice in the realm of digitalization.

References

Abelson, H., Anderson, R., Bellovin, S., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P., Rivest, R., Schiller, J., Schneier, B., Specter, M., & Weitzner, D. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity, 1*(1). https://doi.org/10.1093/cybsec/tyv009

Albers, M. (2005). *Informationelle Selbstbestimmung*. Nomos Verlagsgesellschaft. https://www.nomos-elibrary.de/10.5771/9783845258638_1/titelei-inhaltsverzeichnis?page=1

Albers, M. (2014). Realizing the complexity of data protection. In S. Gutwirth, R. Leenes, & P. Hert (Eds.), *Reloading data protection* (pp. 213–235). Springer. https://doi.org/10.1007/978-94-007-7540-4_11

Ameno, F. (2022, March 21). Ministério da Justiça equipa polícias para vasculhar celulares em troca de dados. *The Intercept Brasil*. https://www.intercept.com.br/2022/03/21/ministerio-da-justica-equipa-policias-para-vasculhar-celulares-em-troca-de-dados/

Anstis, S. (2021). Government procurement law and hacking technology: The role of public contracting in regulating an invisible market. *Computer Law and Security Review, 41*. https://doi.org/10.1016/j.clsr.2021.105536

Anstis, S. (2023). Regulating transnational dissident cyber espionage. *International and Comparative Law Quarterly, 73*(1), 259–274. https://doi.org/10.1017/S0020589323000532

Arantes, R. B. (1999). Direito e política: O Ministério Público e a defesa dos direitos coletivos. *Revista Brasileira de Ciências Sociais, 14*(39). https://doi.org/10.1590/S0102-69091999000100005

Arguição de Descumprimento de Preceito Fundamental n. 1143. (2024). *Amicus Curiae Brief of the Brazilian Institute of Criminal Sciences (IBCCRIM)*. https://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=6900814

Autoridade Nacional de Proteção de Dados. (2025). *Conselho Nacional de Proteção de Dados e Privacidade*. https://www.gov.br/anpd/pt-br/cnpd-2

Badaró, G. (2012). *Processo penal*. Elsevier.

Ball, J. (2013, October 24). NSA monitored calls of 35 world leaders after US official handed over contacts. *The Guardian*. https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security, 1*(2), 178. https://doi.org/10.1017/eis.2016.8

Bellovin, S., Blaze, M., Clarke, S., & Landa, S. (2014). Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. *Journal of Technology and Intellectual Property, 12*(1), Article 1. https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1/

Big Brother Watch. (2016). *Equipment Interference*. https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Equipment-Interference.pdf

Bigo, D., Mc Cluskey, E., & Tréguer, F. (2024). *Intelligence oversight in times of transnational impunity: Who will watch the watchers?* Routledge New Intelligence Studies. https://doi.org/10.4324/9781003354130

Brandão, P. C. (2002). *SNI e Abin: Uma leitura da atuação dos serviços secretos brasileiros ao longo do século XX*. FGV Editora. https://www.academia.edu/43346700/SNI_e_ABIN_uma_leitura_dos_servi%C3%A7os_secretos_brasileiros_ao_longo_do_S%C3%A9culo_XX

Câmara dos Deputados. (2013). *Dispõe sobre a Comissão Mista de Controle das Atividades de Inteligência (CCAI), comissão permanente do Congresso Nacional, órgão de controle e fiscalização externos da atividade de inteligência, previsto no art. 6º da Lei nº 9.883, de 7 de dezembro de 1999*. https://www2.camara.leg.br/legin/fed/rescon/2013/resolucao-2-22-novembro-2013-777449-publicacaooriginal-141944-pl.html

Presidência da República. (1999, December 7). *Comunico a Vossa Excelência que, nos termos do parágrafo 1o do artigo 66 da Constituição Federal, decidi vetar, parcialmente, o Projeto de Lei no 17, de 1999 (no 2.872/97 na Câmara dos Deputados), que "Dispõe sobre o processo e julgamento da arguição de descumprimento de preceito fundamental, nos termos do § 1o do art. 102 da Constituição Federal."* https://www.planalto.gov.br/ccivil_03/leis/Mensagem_Veto/1999/Mv1807-99.htm

Bruneau, T. C. (2015). Intelligence reform in Brazil: A long, drawn-out process. *International Journal of Intelligence and Counterintelligence, 28*(3), 502–519. https://doi.org/10.1080/08850607.2015.1022469

Buermeyer, U., & Mioni, B. (2018, September 9). Gute Lücken, schlechte Lücken? Zur objektiv-rechtlichen Dimension des IT-Grundrechts. *Verfassungsblog*. https://doi.org/10.17176/20180909-151504-0

Bundesamt für Verfassungsschutz. (2024). *Supervision and oversight*. https://www.verfassungsschutz.de/EN/about-us/mission-and-working-methods/supervision-and-oversight/supervision-and-oversight_article.html#doc1021056bodyText5

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. (2020). *Activity report*. https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Taetigkeitsberichte/29TB_20.pdf?__blob=publicationFile&v=3

Bundesverfassungsgericht. (2013). *Order of the First Senate of 24 April 2013 – 1 BvR 1215/07 –, paras. 1-233*. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2013/04/rs20130424_1bvr121507en.html

Bundesverfassungsgericht. (2020). *2020 report*. https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/EN/Jahresbericht/jahresbericht_2020.pdf?__blob=publicationFile&v=6

Bundesverfassungsgericht. (2021). *Constitutional complaint regarding the police's handling of security vulnerabilities in IT systems is inadmissible*. https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2021/bvg21-062.html?nn=148454

Bundesverfassungsgericht. (2022). *Erfolgreiche Verfassungsbeschwerde gegen die Übermittlung mit nachrichtendienstlichen Mitteln erhobener personenbezogener Daten*. https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2022/bvg22-085.html

Bundesverfassungsgericht. (2024). *Activity report*. https://www.bfdi.bund.de/EN/Service/Taetigkeitsberichte/taetigkeitsberichte_node.html

Carpentieri, J. R. (2017). A Abin e o que restou da ditadura: O problema do controle das forças coercitivas do Estado brasileiro. *Dilemas: Revista de Estudos de Conflito e Controle Social, 10*(2). https://revistas.ufrj.br/index.php/dilemas/article/view/10600

Casa Civil, Governo do Brasil. (2023). *ABIN passa a integrar a Casa Civil*. https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/abin-passa-a-integrar-a-casa-civil

Cepik, M. (2020). A *Polícia* Federal, o SISBIN e a *Democracia. Fonte Segura*. https://fontesegura.forumseguranca.org.br/wp-content/uploads/sites/2/2022/04/Ed_37_(Multiplas_vozes)_A-Policia-Federal-o-SISBIN-e-a-Democracia.pdf

Cepik, M. (2021). Intelligence and security services in Brazil: Reappraising institutional flaws and political dynamics. *International Journal of Intelligence, Security, and Public Affairs, 23*(1) pp. 81–102. https://doi.org/10.1080/23800992.2020.1868784

Cepik, M. (2023). *Espionagem e democracia: Agilidade e transparência como dilemas na institucionalização de serviços de inteligência*. Editora Parabellum.

Chaos Computer Club. (2019). *CCC analysiert Münchner Staatstrojaner FinSpy*. https://www.ccc.de/en/updates/2019/finspy

Citizen Lab. (2024). *Pegasus archives*. https://citizenlab.ca/tag/pegasus/

Cohen, J. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.

Cohen, J., & Fung, A. (2021). Democracy and the digital public sphere. In L. Bernholz, H. Landemore, & R. Reich (Eds.), *Digital technology and democratic theory* (pp. 21–56). University of Chicago Press. https://doi.org/10.7208/9780226748603-002

Conectas Direitos Humanos. (2021). *Organizações denunciam irregularidades em licitação para compra de suposta ferramenta de espionagem*. https://www.conectas.org/noticias/organizacoes-denunciam-irregularidades-em-licitacao-do-ministerio-da-justica-para-compra-de-suposta-ferramenta-de-espionagem/

Conselho Nacional de Justiça. (2002). *Justiça em Números 2022: Judiciário julgou 26,9 milhões de processos em 2021*. https://www.cnj.jus.br/justica-em-numeros-2022-judiciario-julgou-269-milhoes-de-processos-em-2021/

Conselho Nacional de Justiça. (2024). *Sistema Nacional de Controle de Interceptações Telefônicas*. https://www.cnj.jus.br/sistemas/sistema-nacional-de-controle-de-interceptacoes-telefonicas/

Council on Ethics. (2022). *Recommendation to exclude Cognyte Software Ltd from investment by the Norwegian Government Pension Fund Global (GPFG)*. https://files.nettsteder.regjeringen.no/wpuploads01/sites/275/2022/12/Rec-Cognyte-ENG.pdf

Council of Europe. (2023). *Pegasus and similar spyware and secret state surveillance*. Committee on Legal Affairs and Human Rights. https://rm.coe.int/pegasus-and-similar-spyware-and-secret-state-surveillance/1680ac7f68

Cunha, P. R. (2010). Militares e anistia no Brasil: Um dueto desarmônico. In V. Safatle & E. Teles (Eds.), *O que resta da ditadura: A exceção brasileira*. Editora Boitempo. https://blogdaboitempo.com.br/wp-content/uploads/2021/05/vladimir-safatle-do-uso-da-violencia-contra-o-estado-ilegal.pdf

Cypher, I., & Neves, R. (2011). Entrevista com Nancy Fraser. In M. A. Abreu (Ed.), *Redistribuição, reconhecimento e representação: Diálogos sobre igualdade de gênero*. Instituto de Pesquisa Econômica Aplicada (IPEA). https://acervo.enap.gov.br/cgi-bin/koha/opac-detail.pl?biblionumber=41601

Dantas, D., & Bronzatto, T. (2024). Abin fez 10 mil consultas informais ao sistema de espionagem FirstMile durante governo Bolsonaro. *O Globo*. https://oglobo.globo.com/politica/noticia/2024/02/24/abin-fez-10-mil-consultas-informais-ao-sistema-de-espionagem-first-mile-durante-governo-bolsonaro.ghtml

Data Privacy Brasil. (2023). *Ofício nº 005/2023 à Procuradoria-Geral da República: Utilização ilícita do sistema FirstMile pela Agência Brasileira de Inteligência*. https://www.dataprivacybr.org/wp-content/uploads/2023/03/Oficio-005.2023.-MPF.-Data-Privacy-Brasil.-Uso-do-FirstMile.pdf

Deutscher Bundestag. (2022). *Fragen zu sogenannter Spionagesoftware* (WD 3-140/22, WD 8-075/22). Wissenschaftliche Dienste. https://www.bundestag.de/resource/blob/924048/ef3dd43c7a11df710a54afe5f794b5c1/WD-3-140-22-WD-8-075-22-pdf.pdf

Deutscher Bundestag. (2024). *Bodies exercising scrutiny*. https://www.bundestag.de/en/committees/bodies/scrutiny

Dutra, L., Rená, P., Vieira, V., & Guilerme, W. (2023). *Hacking governamental: Uma revisão sistemática*. Instituto de Referência em Internet e Sociedade. https://irisbh.com.br/publicacoes/hacking-governamental-uma-revisao-sistematica/

European Parliament. (2023). *Recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware*. https://perma.cc/MB2M-CMTT

Fidler, M. (2015). Regulating the zero-day vulnerability trade: A preliminary analysis. *I/S: A Journal of Law and Policy for the Information Society, 11*(2), pp. 405–483. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2706199

Forbidden Stories. (2024). *The Pegasus Project*. https://forbiddenstories.org/case/the-pegasus-project/

Fouriezos, N. (2022). *Spyware like Pegasus is a warning: Digital authoritarianism can happen in democracies, too*. Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/spyware-like-pegasus-is-a-warning-digital-authoritarianism-can-happen-in-democracies-too/

Franklin, S. B. (2020). *A key part of surveillance reform is now in jeopardy*. Slate. https://slate.com/technology/2020/05/usa-freedom-reauthorization-act-fisa-reform-surveillance-amicus-curiae.html

Fraser, N. (2008). Abnormal justice. *Critical Inquiry, 34*(3), 393–422. https://doi.org/10.1086/589478

Foreign, Commonwealth & Development Office. (2024). *The Pall Mall Process declaration: Tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities*. https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities

Gasser, U., Budish, R., & West, S. M. (2015). *Multistakeholder as governance groups: Observations from case studies*. Berkman Klein Center Research Publication. http://dx.doi.org/10.2139/ssrn.2549270

Gasser, U., Zittrain, J., Olsen, M., O'Brien, D., & Schneier, B. (2016). *Don't panic: Making progress on the "Going Dark" debate*. Berkman Center Research Publication. https://dash.harvard.edu/handle/1/28552576

Gesellschaft für Freiheitsrechte. (2020). *BND law on worldwide mass surveillance*. https://freiheitsrechte.org/en/themen/digitale-grundrechte/bnd-gesetz-2

Gesellschaft für Freiheitsrechte. (2021a). *GFF reicht Datenschutz-Beschwerde ein: Einsatz des Pegasus-Trojaners durch BKA verletzt Grundrechte*. https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-pegasus

Gesellschaft für Freiheitsrechte. (2021b). *GFF erreicht mit Verfassungsbeschwerde gegen Staatstrojaner Grundsatzentscheidung des Bundesverfassungsgerichts für mehr IT-Sicherheit*. https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-grundsatzentscheidung-it-sicherheit

Gomes, F. B. (2010). O modelo alemão de controle de constitucionalidade. *Revista da Faculdade de Direito do Sul de Minas, 26*(2). pp. 153–180. https://www.fdsm.edu.br/adm/artigos/e1ff91a8c7b5ca24065fefa82261ff0b.pdf

Gonçalves, J. B. (2010). Quem vigia os vigilantes? O controle da atividade de inteligência no Brasil e o papel do Poder Legislativo. *Revista de Informação Legislativa, 47*(187), pp. 125–136 https://www2.senado.leg.br/bdsf/item/id/198697

Greco Filho, V. (2012). *Manual de processo penal*. Editora Saraiva.

Habermas, J. (1992). *Between facts and norms: Contributions to a discourse theory of law and democracy*. MIT Press.

Hennessey, S. (2016). Lawful hacking and the case for a strategic approach to "Going Dark." *Brookings*. https://www.brookings.edu/articles/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/

Herpig, S. (2018). *Governmental vulnerability assessment and management: Weighing temporary retention versus immediate disclosure of 0-day vulnerabilities*. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/vulnerability_management.pdf

Herpig, S., & Schwarz, A. (2019). *The future of vulnerabilities equities processes around the world*. Lawfare. https://www.lawfaremedia.org/article/future-vulnerabilities-equities-processes-around-world

Hummel, S., Pfirter, L., & Strachwitz, R. G. (2022). *Civil society in Germany: A report on the general conditions and legal framework*. Maecenata Institut für Philanthropie und Zivilgesellschaft. https://www.ssoar.info/ssoar/handle/document/80687

Instituto Brasileiro de Ciências Criminais. (2009). *Manifestação do assistente técnico e a reforma do Código de Processo Penal: Meio de prova atípico*. Procedimento. https://www.ibccrim.org.br/noticias/exibir/4707/

Ishad, V., & Franco, P. (2008). Os acervos dos órgãos federais de segurança e informações do regime militar no Arquivo Nacional. *Arquivo Nacional, Acervo Rio de Janeiro, 21*(2), pp. 29–42. https://bczm.ufrn.br/comissaodaverdade/ASI%20-%20(CAIXA%2001)/ARTIGOS/Os%20Acervos%20dos%20%C3%93rg%C3%A3os%20Federais%20de%20Seguran%C3%A7a%20e%20Informa%C3%A7%C3%B5es%20do%20Regime%20Militar%20no%20Arquivo%20Nacional.pdf

Kaye, D. (2019). *UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools*. United Nations: Special Rapporteur on Freedom of Opinion and Expression. https://www.ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance

Kaye, D. (2021). The spyware state and the prospects for accountability. *Global Governance, 27*(4). pp 1 – 11. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3990249

Kniep, R. (2024). Code of silence. In D. Bigo, M. McCluskey, & F. Tréguer (Eds.), *Intelligence oversight in times of transnational impunity: Who will watch the watchers?* (pp. 98 – 129). Routledge. https://doi.org/10.4324/9781003354130-4

Kniep, R., Ewert, L., Reyes, B. L., Tréguer, F., McCluskey, M., & Aradau, C. (2023). Towards democratic intelligence oversight: Limits, practices, struggles. *Review of International Studies, 50*(1), pp. 209 – 229. https://doi.org/10.1017/S0260210523000013

Knight First Amendment Institute. (2022). *El Faro journalists, Knight Institute sue NSO Group over spyware*. Knight First Amendment Institute at Columbia University. https://knightcolumbia.org/content/el-faro-journalists-knight-institute-sue-nso-group-over-spyware

Krieger, W. (2010). The German Bundesnachrichtendienst (BND): Evolution and current policy issues. In L. Johnson (Ed.), *The Oxford Handbook of National Security Intelligence*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780195375886.003.0047

Kurz, C. (2023). *Staatstrojaner-Varianten sind eine Fiktion*. Netzpolitik. https://netzpolitik.org/2023/spionagesoftware-staatstrojaner-varianten-sind-eine-fiktion/

Lubin, A. (2023). *Regulating commercial spyware* (The Digital Social Contract: A Lawfare Paper Series). Lawfare. https://www.lawfaremedia.org/article/regulating-commercial-spyware

Mann, S., Nolan, J., & Wellman, B. (2023). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Foucault and Panopticism Revisited, 1*(3), pp. 331–355. https://doi.org/10.24908/ss.v1i3.3344

Mazzilli, H. N. (2022). Democracia: O papel do Ministério Público Brasileiro. *Revista Jurídica da Escola Superior do Ministério Público de São Paulo, 21*, pp. 20–48. https://es.mpsp.mp.br/revista_esmp/index.php/RJESMPSP/article/view/511

McKune, S., & Deibert, R. (2017). *Who's watching little brother? A checklist for accountability in the industry behind government hacking*. Citizen Lab. https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf

Meister, A. (2018). *ZITiS baut Supercomputer zur Entschlüsselung*. Netzpolitik. https://netzpolitik.org/2018/36-millionen-euro-zitis-baut-supercomputer-zur-entschluesselung/

Meister, A. (2023). *Bundesregierung will Hacker-Behörde ausbauen*. Netzpolitik. https://netzpolitik.org/2023/zitis-gesetz-bundesregierung-will-hacker-behoerde-ausbauen/

Menke, F. (2019). A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In G. F. Mendes, I. W. Sarlet, & A. Z. P. Coelho (Eds.), *Direito, inovação e tecnologia* (pp. 781–809). Editora Saraiva. https://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf

Motoryn, P. (2024). *Militares tentam aproveitar crise na Abin para criar órgão de segurança cibernética ligado ao GSI*. The Intercept Brasil. https://www.intercept.com.br/2024/01/31/militares-crise-abin-orgao-de-seguranca-cibernetica-gsi/

Newman, L. (2024). *How leaked NSA spy tool 'EternalBlue' became a hacker favorite*. Wired. https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/

Olliveira, C. (2023). *Na segurança pública, entre direita e essa esquerda, estamos todos fodidos*. The Intercept Brasil. https://www.intercept.com.br/2023/10/10/na-seguranca-publica-entre-direita-e-essa-esquerda-estamos-todos-fodidos/

Peron, I., Shinohara, G., Pereira, G., & Pimenta, G. (2024). *Abin teria sido usada para beneficiar filhos de Abin, afirma PF*. Valor Econômico. https://valor.globo.com/politica/noticia/2024/07/11/pf-deflagra-nova-fase-de-operao-contra-produo-de-notcias-falsas.ghtml

Pfefferkorn, R. (2018). *Security risks of government hacking*. Center for Internet and Society at Stanford University. https://cyberlaw.stanford.edu/publications/security-risks-government-hacking

Ramiro, A., Amaral, P., Canto, M., & Pereira, M. C. (2022). *Mercadores da insegurança: Conjuntura e riscos do hacking governamental no Brasil*. Instituto de Pesquisa em Direito e Tecnologia do Recife. https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf

Ramiro, A. (2024). *Sigilo versus prestação de contas? A Abin e a regulação de tecnologias de monitoramento secreto no STF*. Agenda Estado de Derecho. https://agendaestadodederecho.com/sigilo-versus-prestacao-de-contas-a-abin-e-a-regulacao-de-tecnologias-de-monitoramento-secreto-no-stf/

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. *International Theory, 7*(3), 572–616. https://doi.org/10.1017/S1752971915000081

Real World Crypto Symposium. (2024). *Homepage*. https://rwc.iacr.org/index.html

Rebello, A. (2020). *Conheça o Córtex, sistema de vigilância do governo que integra de placa de carro a dados de emprego*. The Intercept Brasil. https://www.intercept.com.br/2020/09/21/governo-vigilancia-cortex/

Reinke, B. (2020). *Rights reaching beyond borders*. Verfassungsblog. https://doi.org/10.17176/20200531-013615-0

Richter, A. (2024). *PF diz que Abin atuou ilegalmente em favor de filhos de Bolsonaro*. Agência Brasil. https://agenciabrasil.ebc.com.br/geral/noticia/2024-07/pf-diz-que-abin-atuou-ilegalmente-em-favor-de-filhos-de-bolsonaro

Rogaway, P. (2015). *The moral character of cryptographic work*. University of California – Davis. https://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf

Roller, S. M., Wetzling, T., Kniep, R., & Richter, F. (2023). Civic intelligence oversight: Practitioners' perspectives in France, Germany, and the UK. *Surveillance & Society, 21*(2), pp. 189–204. https://doi.org/10.24908/ss.v21i2.15217

Ruschemeier, H. (2022). Die Entwicklung des informationellen Trennungsprinzips. *Verfassungsblog*. https://doi.org/10.17176/20220513-182322-0

Sarlet, I. W., G. B. W. (2020). *Separação informacional de poderes no direito constitucional brasileiro*. Associação Data Privacy Brasil de Pesquisa. https://www.dataprivacybr.org/wp-content/uploads/2022/09/DataPrivacy.-Separacao-Informacional-de-Poderes.-2022.pdf

Sarlet, I. W., Marinoni, L. G., & Mitidiero, D. (2020). *Curso de direito constitucional* (9th ed.). Editora Saraiva.

Schafer, B., & Abel, W. (2010). The German Constitutional Court on the right in confidentiality and integrity of information technology systems. In M. V. Madhuri (Ed.), *Hacking: A legal quandary*. pp. 167–191. ICFAI University Press. https://doi.org/10.2966/scrip.060109.106

Scheppele, K. L. (2024). *Democracy at risk – The autocrat's spyware*? Humboldt Institute for Internet and Society. https://www.youtube.com/watch?v=mhPR6jsx0uU

Schertel, L. (2020). Autodeterminação informativa: A história de um conceito. *Pensar: Revista de Ciências Jurídicas, 25*(4), pp. 1–18. https://doi.org/10.5020/2317-2150.2020.10828

Schneier, B., & Penney, J. (2022). Platforms, encryption, and the CFAA: The case of WhatsApp v. NSO Group. *Berkeley Technology Law Journal, 36*(101), pp. 469–510. https://doi.org/10.15779/Z384B2X554

Schulze, M. (2020). The state of cyber arms control: An international vulnerabilities equities process as the way to go forward? *Sicherheit und Frieden/Security and Peace, 38*(1), 17–21. https://doi.org/10.5771/0175-274X-2020-1-17

Silva, F. (2021). Privacidade e patologias democráticas: Habermas e os desafios da democracia radical. *Doispontos, 18*(2), pp. 22–41. https://revistas.ufpr.br/doispontos/issue/download/3078/845

Superior Tribunal de Justiça. (2021). *Diligências policiais: O que é lícito na investigação, segundo a jurisprudência do STJ*. https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/12092021-Diligencias-policiais-o-que-e-licito-na-investigacao--segundo-a-jurisprudencia-do-STJ.aspx

Supremo Tribunal Federal. (2023a). *PGR questiona no STF falta de regulamentação de monitoramento secreto de celulares e tablets*. https://noticias.stf.jus.br/postsnoticias/pgr-questiona-no-stf-falta-de-regulamentacao-de-monitoramento-secreto-de-celulares-e-tablets/

Supremo Tribunal Federal. (2023b). *STF mantém resolução que disciplina atuação do MP nas interceptações telefônicas*. https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=513469&ori=1

Supremo Tribunal Federal. (2020a). *Arguição de Descumprimento de Preceito Fundamental (ADPF) n. 403: Voto Ministro Edson Fachin*. https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf

Supremo Tribunal Federal. (2020b). *STF impõe limites ao compartilhamento de dados do Sistema Brasileiro de Inteligência (Sisbin)*. https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=449549&ori=1

Supremo Tribunal Federal. (2021). *STF confirma limitações ao compartilhamento de dados do Sisbin*. https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=474835&ori=1#:~:text=STF%20confirma%20limita%C3%A7%C3%B5es%20ao%20compartilhamento,o%20interesse%20p%C3%BAblico%20da%20medida

Supremo Tribunal Federal. (2022). *STF julga inconstitucionais atos do Ministério da Justiça sobre dossiês contra antifascistas*. https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=487103&ori=1

Quinlan, S., & Wilson, A. (2016). *A brief history of law enforcement hacking in the United States*. New America. https://na-production.s3.amazonaws.com/documents/History_Hacking.pdf

Teixeira, L. (2020). *O que é, quem fez e quem está no dossiê antifascista*. UOL. https://noticias.uol.com.br/politica/ultimas-noticias/2020/08/18/uol-explica-o-que-e-quem-fez-e-quem-atinge-o-dossie-antifascista.htm

Thompson, A. W. (2021). *Assessing the Vulnerabilities Equities Process, three years after the VEP Charter*. Lawfare. https://www.lawfaremedia.org/article/assessing-vulnerabilities-equities-process-three-years-after-vep-charter

United Nations. (2013). *Brazil and Germany – draft resolution: The right to privacy in the digital age. General Assembly. Third Committee: Promotion and protection of human rights: Human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms*. https://www.auswaertiges-amt.de/blob/258452/83ab86266ce693fd2b184bdaaf3c0a61/131127-right2privacy-en-data.pdf

Valente, R. (2023). *O "monstro" renasceu na Abin sem nenhum controle do Congresso*. Agência Pública. https://apublica.org/2023/10/o-monstro-renasceu-na-abin-sem-nenhum-controle-do-congresso/

Vergili, G. (2022). *Tecnoautoritarismo e o controle das atividades de inteligência: Por que a CCAI não está analisando mais casos*? Associação Data Privacy Brasil de Pesquisa. https://www.dataprivacybr.org/documentos/tecnoautoritarismo-e-o-controle-das-atividades-de-inteligencia-por-que-a-ccai-nao-esta-analisando-mais-casos/?idProject=

Wetzling, T. (2017). *Germany's intelligence reform: More surveillance, modest restraints and inefficient controls*. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf

Wetzling, T (2023a). Intelligence oversight collaborationin Europe. In D. Bigo, M. McCluskey, & F. Tréguer (Eds.), *Intelligence oversight in times of transnational impunity: Who will watch the watchers*? (pp. 254 – 262). Routledge. https://www.doi.org/10.4324/9781003354130-10

Wetzling, T. (2023b). *National security surveillance in Germany*. Safe and Free: National Security Surveillance and the Rule of Law Across Democratic States. https://safeandfree.io/paper/national-security-surveillance-in-germany/

Wikileaks. (2017). *Vault 7: CIA Hacking Tools Revealed*. https://wikileaks.org/ciav7p1/

Wills, A., & Vermeulen, M. (2011). *Parliamentary oversight of security and intelligence agencies in the European Union*. European Parliament - Citizens' Rights and Constitutional Affairs - Justice, Freedom, and Security. https://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf

Zaffaroni, E. R. (2007). A esquerda tem medo, não tem política de segurança pública. *Revista Brasileira de Segurança Pública, 1*(1), pp. 130 – 139. https://revista.forumseguranca.org.br/index.php/rbsp/article/view/36/34

Zaverucha, J. (2008). De FHC a Lula: A militarização da Agência Brasileira de Inteligência. Política Hoje. *Revista de Sociologia e Política, 16*(31), pp. 177 – 195. https://doi.org/10.1590/S0104-44782008000200013

Zaverucha, J. (2010). Relações civil-militares: O legado autoritário da Constituição Brasileira de 1988. In V. Safatle & E. Teles (Eds.), *O que Resta da Ditadura: A Exceção Brasileira* (pp. 187 – 208). Editora Boitempo.

Zegart, A. (2000). *Flawed by design: The evolution of the CIA, JCS, and NSC*. Stanford University Press.

Zegart, A. (2011). *Eyes on spies: Congress and the United States intelligence community*. Hoover Institution Press.

Zegart, A. (2022). *Spies, lies, and algorithms: The history and future of American intelligence*. Princeton University Press.

Zvi, R. R. (2023). *Managing risky business: The international regulatory framework of spyware companies: Where it is lacking and where it is heading*. Georgetown Law - Center on Transnational Business and the Law. https://www.law.georgetown.edu/ctbl/blog/managing-risky-business-the-international-regulatory-framework-of-spyware-companies-where-it-is-lacking-and-where-it-is-heading/

Acknowledgement

This paper is the result of a research fellowship at the Weizenbaum Institute, for whose support and trust I am immensely grateful. I would like to acknowledge the more than valuable contributions of Clara Keller, Ronja Kniep, and all the members of the "Technology, Power, and Domination" research group, especially during the Fellows Colloquium at the Berlin Social Sciences Center where the initial results of this investigation were first presented and discussed. My thanks also go to the Alexander von Humboldt Institute for Internet and Society, especially to Jörg Pohle, who has followed and helped to unravel the challenges of comparative research in this field, sowing the initial ideas for this endeavor. I also thank the peer reviewers for their thorough reading and generous comments, which contributed to the final, improved version of the paper.

Date received: August 2024
Date accepted:April 2025