REVISTA DIREITO MACKENZIE

ISSN 2317-2622 | RDM | Revista Direito Mackenzie | São Paulo | SP | 19(3) | e18056EN | 2025
http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056EN

SECURITY INCIDENTS, DATA LEAKS AND CYBER ATTACKS: POSSIBLE ANSWERS FOR THE APPLICATION OF THE LAW BASED ON THE STJ'S DECISIONS IN RESP 2.147.374/SP AND ARESP 2.130.619/SP

RECEIVED:	JUN. 9TH, 2025
ACCEPTED:	OCT. 23TH, 2025

Gabriel Cemin Petry

https://orcid.org/0000-0002-2357-1573
Universidade do Vale do Rio dos Sinos (Unisinos)
Novo Hamburgo, RS, Brasil
E-mail: Gabrielcpetry96@gmail.com

Karin Regina Rick Rosa

https://orcid.org/0009-0001-2530-951X
Universidade do Vale do Rio dos Sinos (Unisinos)
Novo Hamburgo, RS, Brasil
E-mail: karinrick.rosa@gmail.com

Wilson Engelmann

https://orcid.org//0000-0002-0012-3559
Universidade do Vale do Rio dos Sinos (Unisinos)
Novo Hamburgo, RS, Brasil
E-mail: wengelmann@unisinos.br

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056EN
2025 | v. 19 | n. 3 | p. 1-24 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056EN

· GABRIEL CEMIN PETRY
· KARIN REGINA RICK ROSA
· WILSON ENGELMANN

How to cite this article: PETRY, G. C.; ROSA, K. R. R.; ENGELMANN, W. Security incidents, data leaks and cyber attacks: possible answers for the application of the law based on the STJ's decisions in REsp 2.147.374/SP and AREsp 2.130.619/SP. *Revista Direito Mackenzie*, São Paulo, SP, v. 19, n. 3, e18056EN, 2025. http://dx.doi.org/10.5935/2317-2622/direito-mackenzie.v19n318056EN

ABSTRACT: The central problem of the study is to verify how the STJ has applied the law in cases involving security incidents, such as data leaks and cyber attacks, considering the multiplicity of forms, agents and different impacts that such incidents can have. The aim is to analyze the concepts of security incidents and investigate how the STJ has applied the law in two precedents, REsp 2.147.374/SP and AREsp 2.130.619/SP. To this end, the deductive research method is adopted, based on bibliographical, documentary and jurisprudential research. Based on the cases studied, it is concluded that there are conceptual inconsistencies arising from a possible generalization of the term security incidents, a circumstance that can hinder the application of the law. It is necessary to improve the technical understanding of security incidents, their differentiation, as well as recognizing risk as a relevant element for civil liability, corroborating the consolidation of practices consistent with the LGPD.

KEYWORDS: Digital Law; cybersecurity; data protection.

INCIDENTES DE SEGURANÇA, VAZAMENTO DE DADOS E ATAQUES CIBERNÉTICOS: POSSÍVEIS RESPOSTAS PARA APLICAÇÃO DO DIREITO A PARTIR DAS DECISÕES DO STJ NO RESP 2.147.374/SP E ARESP 2.130.619/SP

RESUMO: O problema central do estudo é verificar como o STJ tem aplicado o Direito diante de casos envolvendo incidentes de segurança, como vazamento de dados e ataques cibernéticos, considerando a multiplicidade de formas, agentes e diferentes impactos que tais acontecimentos podem alcançar. Busca-se analisar os conceitos de incidentes de segurança, além de investigar como o STJ aplicou o Direito em dois precedentes, o REsp 2.147.374/SP e AREsp 2.130.619/SP. Para tanto, adota-se o método de investigação dedutivo, pautado em pesquisa bibliográfica, documental e jurisprudencial. A partir dos casos estudados,

conclui-se que existem inconsistências conceituais, que decorrem de uma possível generalização do termo incidentes de segurança, circunstância que pode prejudicar a aplicação do Direito. É necessário aprimorar a compreensão técnica dos incidentes de segurança, sua diferenciação, além de reconhecer o risco como elemento relevante à responsabilização civil, corroborando para consolidação práticas coerentes com a LGPD.

PALAVRAS-CHAVE: Direito Digital; cibersegurança; proteção de dados.

1. Introduction

In recent decades, digital transformation has exponentially intensified the circulation of data and human dependence on information systems in all sectors of society, in contrast, broadening the risks associated with their security. In this context, security incidents, especially data leaks and cyber attacks, have become recurrent and high-impact events, requiring normative, technical, and institutional responses that are commensurate with the complexity of the problem. These events not only compromise digital and operational assets but also affect fundamental rights, such as privacy, informational self-determination, and notably, the protection of personal data.

The present investigation fits into this scenario, and its central problem lies in verifying how the STJ has applied the law in cases involving security incidents, such as data leaks and cyber attacks, considering the multiplicity of forms, agents, and different impacts that such incidents can assume. The proposed approach thus seeks to clarify the distinct legal and technical concepts involved - security incidents, cyber attacks, and data leaks - in order to contribute to overcoming possible terminological confusions in legal discourse and judicial decisions. The analysis is justified by the urgency of consolidating a precise and technically grounded understanding of these occurrences, with a view toward the effective protection of rights in the digital ecosystem.

The article aims to conceptualize and distinguish the variations of the so-called security incidents, including cyber attacks and data leaks, examining their possible causes, effects, and legal implications - a conceptual delimitation that is fundamental to clarifying the distinct technical and regulatory concepts, aiming to contribute to overcoming possible terminological confusions in legal discourse and judicial decisions. Subsequently, the aim is to analyze how the STJ has applied the law in cases involving

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056EN
2025 | v. 19 | n. 3 | p. 1-24 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056EN

security incidents, utilizing the examination of two decisions: REsp 2.147.374/SP and AREsp 2.130.619/SP.

The choice of STJ rulings is justified by the need to verify the varied responses of the Superior Court to the multiplicity of security incidents and their impacts. The joint examination of these precedents uncovers nuances and divergences regarding the application of the Law, because while REsp 2.147.374/SP speaks of objective and proactive liability, AREsp 2.130.619/SP aligns with the traditional subjective logic regarding the proof of effective damage. The critical analysis of the precedents allows for the examination of conceptual inconsistencies and the possible generalization of the term "security incidents" in legal discourse, which can hinder the application of the Law and the effective protection of users, consumers, and data subjects.

To this end, a deductive methodological approach of an exploratory nature is adopted, subsidized by documentary and bibliographical research. It thus starts from general knowledge, with the conceptual delimitation and distinction of the variations of the term "security incident," based on legislation, specialized doctrine, and regulations from the National Data Protection Authority (ANPD), to then arrive at the particular, which is to analyze and explain how the law was applied in two specific judicial cases (REsp 2.147.374/SP and AREsp 2.130.619/SP) by the STJ. The deductive reasoning thus makes it possible to *(i)* verify whether the STJ's decisions are logically coherent with the established general premises and *(ii)* analyze whether there are conceptual inconsistencies in the application of the Law and/or the generalization of the term "security incidents" in legal discourse.

The first section proposes a conceptual delimitation of security incidents, presenting the technical foundations that characterize them and differentiating them from cyber attacks and data leaks. This section also analyzes provisions of the General Data Protection Law (LGPD) and ANPD regulations that touch upon the subject of security incidents. The second section, finally, examines the STJ rulings, seeking to identify how the court dealt with the concept of security incidents, and, among other factors, what criteria were used to assess the liability of data processing agents, in order to verify what challenges emerge for the characterization of damage in contexts of digital risk.

The proposed structure thus allows for an integrated and critical understanding of the multiple dimensions involved in security incidents, serving as a subsidy for improving legal action in the face of new technological dynamics. In the end, the intent

is not only to offer a brief and incipient theoretical systematization on the topic but also to foster a propositional reflection on the need for jurisprudential and regulatory evolution compatible with the complexity of the digital era.

2. Security incidents: data leaks, cyber attacks, and other concepts for the application of law

Initially, as clarified by Carvalho and Souza (2019, p. 155), it became popularly conventional to call any type of problem related to the so-called "security incidents" a "data leak," when incidents have a much broader spectrum than a security breach. The concepts, however, differ in their definition and may have distinct consequences, including for the interpretation and application of the law. In this section, three relevant terminologies in the context of digital law will be addressed: *(i)* security incidents; *(ii)* data leaks; and *(iii)* cyber attacks.

2.1 Security incidents

Security incidents are those that affect information security, so before discussing their concept, it is necessary to address information security, which, incidentally, is a long-standing concern, as security methods have long been used to prevent unauthorized access to information. It is worth remembering that the first computer was created to break the security mechanism used by Germany in World War II. The mathematical models created for data confidentiality, called cryptography, have evolved with technology, but information security has not kept pace with this advancement, so vulnerabilities have begun to grow, a circumstance that persists due to the increasing complexity and intensity with which computer systems integrate objects, networks, and environments (Schneier, 2019, p. 26-28).[1] The advent of cybercrime, for example, has caught the attention of regulators and legislators, and the combination of stronger legislation and more aggressive cyber attacks has changed the information security landscape for organizations (Freire *et al.*, 2024).

1 According to Schneier, the complexity of computer systems means that it is easier to attack than to defend, since complex systems imply, at least in principle, a greater area for exploiting vulnerabilities, especially considering the interoperability and interconnection between systems (Schneier, 2019, p. 26-28).

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056EN
2025 | v. 19 | n. 3 | p. 1-24 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056EN

Information security is a vital part of business and is achieved through the implementation of an appropriate set of controls, which include policies, processes, procedures, organizational structures, as well as software and hardware functions. To effectively protect assets, it is necessary to protect the *confidentiality*, *integrity*, and *availability* of data, and this is done through controls that are established, implemented, monitored, reviewed, and constantly improved.[2]

The fundamental principles of information security are *confidentiality*, *integrity*, and *availability*[3] (Hintzbergen *et al.*, 2018, p. 20), serving as a starting point for understanding security incidents. Confidentiality, also known as exclusivity, relates to limiting who can obtain information:

> Confidentiality ensures that the necessary level of secrecy is applied to each element of data processing and prevents unauthorized disclosure. This level of confidentiality must prevail while the data resides in systems and devices on the network, when it is transmitted, and when it reaches its destination (Hintzbergen *et al.*, 2018, p. 21).

Integrity refers to the consistency and accuracy of information, meaning that it is complete, perfect, and intact. Any unauthorized modification of data, whether intentional or not, violates the principle of integrity. Availability is characterized by access to information when needed and continuity of work in the event of failure. Based on these three basic principles, it is also possible to outline three types of security incidents:

> The first of these, confidentiality incidents, covers occurrences in which there is accidental or unauthorized disclosure of or access to personal data. Integrity incidents occur when there is some type of accidental or unauthorized alteration of data. Finally, availability incidents are those in which there is accidental or unauthorized loss of access or destruction of such data (Luciano, 2019, p. 164).

2 ISO 27002:2013, superseded by ISO/IEC 27002:2022, addresses the process for information security management - Code of practice for information security - highlighting the importance of understanding information security requirements, implementing and operating controls to manage information security risk, monitoring and reviewing the performance and efficiency of the Information Security Management System, and improving based on objective measurements. Available at: https://www.iso.org/standard/75652.html. Access on: May 4, 2025.

3 Known as the "CIA" triangle (Hintzbergen *et al.*, 2018, p. 20).

It is worth mentioning that, in addition to these three fundamental principles, there are three others that form the so-called Parkerian Hexagram. They are: *ownership or control*, *authenticity*, and *usefulness*. Anything that affects one or more of these fundamental attributes of information can characterize a security breach (Hintzbergen *et al.*, 2018, p. 27).

Threats to information security can be human or non-human. In the category of human threats, we have those that are intentional, such as an attack by a hacker, an employee who, after being fired, destroys data, or reveals information to competitors. Social engineering is another example of an intentional human threat, which works by exploiting a lack of security awareness. Unintentional human threats, on the other hand, result from accidents that can happen, such as data deletion or the installation of a virus (malware) from an email message (e.g., phishing attacks). On the other hand, there are situations that do not involve human actions, such as electrical discharges, fires, and floods, among others. These threats can result in direct or indirect damage, and it is necessary to deal with the risks by accepting, mitigating, and avoiding them as much as possible.

Thus, security incidents can be defined as "a single or series of unwanted or unexpected information security events that are highly likely to compromise an organization's business operations" (Carvalho; Souza, 2019, p. 155)[4]. From this perspective, "the loss of a flash drive, the theft of a laptop, or the interruption of access to a system can be considered security incidents from a technical point of view, as corporate information will be exposed to a threat" (Jimene, 2019, RL.1.14). The term "security incident" (or simply "incident") appears six times in the text of the General Data Protection Law (Lei Geral de Proteção de Dados - LGPD), specifically in Chapter VII, Sections I and II, without being effectively defined or conceptualized in the list of nineteen items in Article 5 of the special legislation (Luciano, 2019, 164).[5]

The National Data Protection Authority (ANPD), through Resolution CD/ANPD No. 15, of April 24, 2024, which approved the "Security Incident Communication Regulation," in its Article 3, item XII, accepted the concept already established in

4 In addition to the security incident, another relevant term is "anomaly," which can be identified as a "pre-incident" phase. If confirmed, the 'anomaly' becomes a real "incident" (Carvalho; Souza, 2019, p. 155).

5 The LGPD uses indeterminate legal concepts at various points when it refers to "appropriate security measures" and "security incidents," which is why refining the concepts through risk assessments, considering specific cases (nature of the incident, types of data involved, and severity of the consequences) seems welcome (Luciano, 2019, p. 164).

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056EN
2025 | v. 19 | n. 3 | p. 1-24 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056EN

information security. In this sense, a security incident is "any confirmed adverse event related to the violation of the properties of confidentiality, integrity, availability, and authenticity of personal data security" (ANPD, 2024). In other words, the term security incident (in this case, of personal data), conceived as "any adverse event," seems to lead to a comprehensive concept, like an "umbrella" that includes several possibilities (e.g., both the invasion of a mobile device and the theft of confidential documents can constitute examples of security incidents).

Two other important definitions appear in the regulation: *(i)* "incident that may cause significant risk or damage," and; *(ii)* "large-scale data incident." The first, strictly speaking under Article 5 and its subparagraphs, occurs when the incident affects the fundamental interests and rights of data subjects and, cumulatively, involves any of the following types of data: sensitive personal data, data on children, adolescents, or the elderly; financial data; system authentication data; data protected by tax, legal, or professional secrecy. The second, in turn, is defined as "one that covers a significant number of data subjects, also considering the volume of data involved, as well as the duration, frequency, and geographical extent of the data subjects' location" (ANPD, 2024).

Once a relevant incident (within the parameters of the LGPD) has been confirmed, there is a duty to notify - an indispensable element in the incident handling process, as required by Article 48 of the LGPD. Its importance is multifaceted and ranges from detection and prevention to contributing to collective security on the internet and generating knowledge (ANPD, 2022). It is reiterated: a personal data security incident, as defined, is any adverse and confirmed event related to a breach in personal data security, which may involve unauthorized access, destruction, loss, leakage, or improper processing that jeopardizes the rights of data subjects. The leakage of personal data, being a critical type of incident, is characterized by the obtaining and exposure of such data, often affecting many data subjects, so here is a point of utmost importance for reflection on the relevant role of notification.

The importance of notification lies, first and foremost, in improving the ability to detect incidents. Many institutions only discover that they have been compromised when notified by third parties; a 2021 report indicated that 41% of compromise victims learned of the problem through external notification. Notification, therefore, can contribute to the identification of problems and the prevention of new occurrences for both the notifier and the notified party.

In addition to detection and prevention, notification contributes to overall Internet security, because when notifying an attempted attack of which it was a victim, the entity must not only mitigate the immediate damage but also seek to solve the cause of the problem, demonstrating a commitment to cybersecurity issues. This is crucial to contain damage and losses, especially in cases of fraud.

From a regulatory standpoint, reporting security incidents is also an obligation for the controller in certain cases. The ANPD receives reports of security incidents, which must be detailed and accompanied by documents, in addition to incident reports, whenever relevant data of data subjects is involved. In fact, a large part of the sanctioning proceedings finalized at the administrative level by the authority involve "Failure to report security incidents to the ANPD and data subjects" (ANPD, 2025). The report and documentation enable the ANPD to understand the severity and assess the measures taken to mitigate the risks. This demonstrates that the importance of notification transcends the technical sphere, extending to compliance with data protection regulations, such as the LGPD.

Furthermore, the consolidation of the information contained in the notifications enables the generation of statistics, the correlation between data, and the identification of trends. This data is valuable for the development of recommendations and support materials, the guidance of campaigns for the adoption of good practices, and the establishment of cooperative actions between different entities and CSIRTs (Computer Security Incident Response Teams).

In order for organizations to monitor and, above all, for those responsible to know how to act in the event of a security incident, it is essential to develop an Incident Response Plan.

2.2 Data leaks

According to the ANPD, data leaks are one of the most well-known security incidents and essentially occur when data is improperly accessed, collected, disclosed, or passed on by third parties. Some of the consequences of a leak include the use of leaked data and information to perpetrate fraud, attempted scams, misuse by third parties, and even the sale of data, situations that are capable of causing damage to data subjects (ANPD, 2022). Despite this, it is worth noting, even due to the inaccuracy in dealing with different types of security incidents and their consequences, that some Brazilian

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056EN
2025 | v. 19 | n. 3 | p. 1-24 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056EN

courts (such as the Court of Justice of the State of São Paulo) do not have fixed bases for determining whether a data leak would be capable of resulting in extra-patrimonial compensation, *in re ipsa*, for example (Oliveira; Gomes; Matteu, 2023, p. 11-25).

Data leaks are a reality in modern societies, with recurring headlines in newspapers and news sites in this regard. The origin of the leaks? They are extremely varied: public, private, and even government organizations, which proves that leaks are not restricted to a particular economic sector or specific activity (Carvalho; Souza, 2019, p. 156). Everyone - individuals, companies, organizations, and governments - is prone to having their data (personal or otherwise) leaked in some kind of security incident. Furthermore, data leaks can imply violations of the right to privacy, data protection, intellectual property, and, among other things, such incidents put people (data subjects, users, consumers) at risk of economic and financial loss and can even tarnish the reputation of those affected (just to cite one example, consider the case of an individual's credit rating being negatively affected by credit protection agencies due to fraudulent contracting made possible by a leak of their personal data).

Furthermore, this type of security incident can occur due to improper access, collection, or disclosure of data, a situation that, in turn, may originate from: a) the invasion of a user's account by an unauthorized person; b) theft of computer devices and equipment; c) human error (usually linked to phishing cases); d) negligence in information security and data processing; and, nevertheless; e) may originate from another type of security incident: the action of hackers in cyber attacks (CERT.br; CGI.br; ANPD, 2024). Cyber attacks, unlike data leaks (as will be seen), can have more catastrophic consequences. After all, as Schneier (2019, p. 9) points out: "now that everything is computerized, threats concern life and property."[6].

The leakage of personal data characterizes a security incident that may affect, jointly or not, the attributes of confidentiality, integrity, and availability.

2.3 Cyber attacks

According to CISCO, the term "cyber attacks" refers to a malicious and deliberate attempt by an individual/organization to breach the information system of another

6 In the original: "Now that everything is a computer, the threats are about life and property." Schneier issues this warning because more and more devices have become "smart things," made "intelligent" through the adoption of networked computing devices that interact with other devices. He cites, as examples, washing machines, cars, and even airplanes, which demonstrates how cyber attacks can have catastrophic consequences (Schneier, 2019, p. 9).

individual/organization in order to obtain some benefit, monetary or otherwise. Sometimes, the attacker's goal or motivation is not financial, but purely activist (hacktivism) or military (Cyber Warfare) (Petry; Huppfer, 2023, p. 89). Among the most common tools used by attackers (hackers) are malware (malicious software), ransomware, spyware, man-in-the-middle attacks (interference in traffic to filter and steal data), DoS or DDoS (attacks to interrupt services) (CISCO, 2017) and, among other examples, social engineering techniques such as phishing and vishing (fraudulent communications that exploit the weakest link in the information security chain: humans) (Silva, 2023, p. 25-31; Petry; Hupffer, 2023, p. 89; Branquinho; Branquinho, 2021, p. 88-99).

The impacts of a cyber attack can be very serious and, from a legal perspective, transcend the criminal sphere—relating to the punishment of cybercriminals for hacking into computer devices, for example. The phenomenon has implications in various areas of law, since it has the power to undermine contractual relationships between individuals, organizations, public and private entities, and even interrupt the provision of public services. It is, therefore, a global issue and one of undeniable public interest, as already noted by the European Parliament in the Cyber Resilience Act, approved on October 23, 2024: "Cyber attacks are a matter of public interest, as they have a critical impact not only on the Union's economy, but also on democracy and the health and safety of consumers" (European Parliament, 2024).

According to the National Cybersecurity Strategy (E-Ciber), the almost total digitization of business models—and of the Digital Government itself—has had beneficial effects on society, as it has boosted the global economy. However, this same digitization process has had the side effect of making society more vulnerable to cyber attacks (Brazil, 2020a). Regarding the possible impacts of a cyber attack, the National Strategy stated:

> In recent cyber attacks, hacker groups have considered government systems as rewarding targets, with the aim of causing various impacts, such as: potential damage to the government's image among its domestic audience and the international community, discrediting public services among the population, undermining international investors' confidence in the public administration's ability to protect its own systems, undermining confidence in electoral processes, and discontent among the population with regard to public administration. In addition to protecting the government itself, another critical issue is the cyber protection of companies representing critical infrastructure. For the sake of understanding, we can

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056EN
2025 | v. 19 | n. 3 | p. 1-24 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056EN

> conceptualize these as facilities, services, and assets that, if interrupted or destroyed, will cause serious social, economic, political, international, or national security impacts. These companies need to have a consistent and evolving approach to cybersecurity to identify and assess vulnerabilities and manage the risk of threats by observing, for example, the five functions provided for in the cybersecurity framework of the National Institute of Standards and Technology (NIST), which are: Identify, Protect, Detect, Respond, and Recover (Brazil, 2020a).

Depending on the type of attack and the target, a cyber attack can naturally be considered a "data protection security incident capable of causing significant risk or damage to data subjects," pursuant to Article 5, §1, of CD/ANPD Resolution No. 15, of April 24, 2024, which occurs when the processing activity may "prevent the exercise of rights or the use of a service, as well as cause material or moral damage to data subjects, such as discrimination, violation of physical integrity, the right to image and reputation, financial fraud, or identity theft" (ANPD, 2024). A *priori*, we can relate this classification to attacks against critical infrastructure, for example, since they concern essential services and activities of society (such as water supply, fuel, electricity, health services, telecommunications, etc.).

Finally, it is no coincidence that one of the guiding principles of the National Cybersecurity Policy and the National Cybersecurity Committee (PNCiber), established by Decree No. 11,856/2023, is "the prevention of cyber incidents and attacks, in particular those directed at critical national infrastructure and essential services provided to society," alongside the protection of fundamental rights and the resilience of public and private organizations to cyber incidents and attacks (Brazil, 2023a). Everyone must be prepared, but critical infrastructure, since, according to the National Critical Infrastructure Security Strategy, "it has a strategic dimension, as it plays an essential role both for national security and sovereignty and for the integration and sustainable economic development of the country" (Brazil, 2020b).

3. Application of law facing security incidents: the case of REsp 2.147.374/SP and AREsp 2.130.619/SP judged by STJ

This section will examine two precedents from the Superior Court of Justice (STJ) that, in their own way, dealt with security incidents: *(i)* Special Appeal No. 2.147.374/SP,

involving a hacker attack and data leak, as mentioned in the summary of the decision, and; *(ii)* Special Appeal No. 2.130.619//SP, filed by Eletropaulo Metropolitana Eletricidade de São Paulo S.A. (ENEL), involving a data leak.

3.1 The case REsp n° 2.147.374/SP

Originally, the plaintiff, the data subject, filed a lawsuit seeking specific performance and compensation for moral damages against Eletropaulo Metropolitana Eletricidade de São Paulo S.A. She claimed that she received a communication from the Institute for the Protection of Personal Data (Iprodape) with news of a security incident involving the leakage of the following personal data: full name, CPF and RG numbers, email address, and telephone numbers. He argued that his privacy had been violated and that, for this reason, compensation for moral damages was due, pursuant to Article 42 of the LGPD. In this case, Eletropaulo did not disclose the circumstances in which the incident occurred or the identity of the third parties who had access to such data.

The claim was dismissed at first instance, and subsequently, the São Paulo State Court of Justice (TJSP) overturned the decision to partially uphold the appeal, recognizing the occurrence of a leak of non-sensitive personal data, without, however, setting compensation for moral damages. However, due to this leak, Eletropaulo was ordered to provide information on the public and private entities with which it shared the data, in addition to providing a complete statement with the origin, the absence of records, the criteria used, and the purpose of the data processing, as well as an exact copy of all data relating to the data subjects contained in its files (Brazil, 2024). .

The premises established in the TJSP ruling were as follows: *(i)* the appellant Eletropaulo was the victim of a hacker attack; *(ii)* as a result of the attack, there was a data leak, exposing the plaintiff's non-sensitive personal data; *(iii)* there was a failure in the provision of services, which requires data processors to adopt security measures; *(iv)* the appellant Eletropaulo was ordered to provide the information requested by the data subject, pursuant to art. 19, inc. II, of the LGPD[7] ; *(v)* there was no order to pay compensation for moral damages, as these were not proven (Brazil, 2024).

7 Art. 19. Confirmation of the existence of or access to personal data shall be provided, upon request by the data subject: II - by means of a clear and complete statement indicating the origin of the data, the absence of records, the criteria used, and the purpose of the processing, observing commercial and industrial secrecy, provided within fifteen (15) days from the date of the data subject's request.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056EN
2025 | v. 19 | n. 3 | p. 1-24 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056EN

The Special Appeal was filed by Eletropaulo, pursuant to Article 103, item I, subitem "a," of the Federal Constitution of 1988, alleging violation of Articles 18, item VII, 19, item II, 42, caput, 43, item III, and 46, caput, of Law 13,709/2018 (LGPD)[8]. It was argued that the obligations contained in Article 18, item VII, and Article 19, item II, refer to the complete declaration in cases of lawful sharing of personal data. However, in this case, it was understood that the sharing would be unlawful, since it would have resulted from a cyber attack. Herein lies the controversy of the appeal: would the leakage of non-sensitive personal data of the data subject, resulting from unlawful activity (cyber attack), be liable to generate the obligations set forth in the LGPD for the data processor? Or, on the other hand, would the fact that the leak occurred as a result of an unlawful activity (cyber attack) be an exclusion from liability, as provided for in Article 43, item III, of the LGPD (e.g., third-party fault)? (Brazil, 2024). In fact, it is questionable whether the exclusive fault of a third party would exempt the processing agent from presenting the information required by Article 19 of the LGPD.

In addressing the issue, the Superior Court of Justice invoked the fundamental right to personal data protection, included in item LXXIX of Article 5 of the Federal Constitution of 1988, through Constitutional Amendment No. 115/2022, noting that the Federal Supreme Court recognized data protection as a fundamental right even before it was codified, according to ADIs 6387, 6388, 6389, 6390, and 6393 MC-REF/DF (DJe 11/12/2020). There was also mention of Special Appeal No. 2.130.619-SP, also dealing with a case of compensation brought against ENEL due to the leakage and access of personal data by third parties – which will be explored further below (Brazil, 2024).

The Superior Court stated that the microsystem introduced by the LGPD created, expanded, and consolidated guidelines for dealing with the issue from the perspective of protecting fundamental rights, in addition to signaling a new system of accountability, called proactive civil liability, as stated by the TJSP and part of the doctrine. It also reiterated some key concepts for the application of the LGPD (Article 5), such as

8 Art. 18. The data subject has the right to obtain from the controller, in relation to the data processed by him, at any time and upon request: VII - information on the public and private entities with which the controller has shared data;
Art. 43. Processing agents shall not be held liable only when they prove: III - that the damage is due to the exclusive fault of the data subject or a third party.
Art. 46. Processing agents must adopt security, technical, and administrative measures capable of protecting personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication, or any form of inappropriate or unlawful processing.

data subject, controller, operator, and processing agents, outlining the legal contours of those involved in the "data protection ecosystem"[9].

Upon verifying that Eletropaulo would fall within the category of processing agent, the Superior Court understood that it would be incumbent upon it, as a processing agent, to take all security measures expected by the data subject, also stating that the systems used for processing must be structured in such a way as to meet the security requirements, standards of good practice, governance, and principles enshrined in the text of the LGPD. In other words: "the legislation suggests a series of procedures, tools, and conduct to be followed by processing agents in order to prevent security incidents" (Brazil, 2024). Regarding cyber attacks and data leaks, it was stated:

> With regard to the alleged security incident (hacker attack), it should be noted that cyber attacks aimed at identifying security vulnerabilities in various systems and obtaining as much data as possible are becoming increasingly frequent. Data breaches or leaks consist of situations in which a large volume of personal information (such as name, address, document numbers, bank details, access credentials, among others) is extracted, resulting in consequences for its owners, depending on the extent of the attack. In the long term, the lack of elements capable of ensuring information security can lead to a real erosion of privacy, in which sensitive data related to individuals' identities can be misappropriated by third parties on a continuous and indeterminate basis (Brazil, 2024).

In reality, cyber attacks are not essentially intended to "identify vulnerabilities," but rather to exploit vulnerabilities that already exist or have been identified by attackers, vulnerabilities that may arise from either negligence or deliberate omission on the part of data processors, for example. Furthermore, even regarding the purposes of the attack, they will not always be aimed at "obtaining as much data as possible," just as the consequences, as seen above, can vary depending on the type of attack, target, and objective of the attacker. Such statements only demonstrate the need to disseminate and expand knowledge on the complex issues of cybersecurity and information security (especially in view of the harmful potential that security incidents can cause to legal relationships). Treating the topic of security incidents (whether data leaks or cyber

9 To address proactive civil liability, based on the concept of accountability, the decision refers to: QUEIROZ, João Quinelato de; MORAES, Maria Celina Bodin de. Autodeterminação informativa e responsabilização proativa. *Cadernos Adenauer XX*, nº 3, 2019, p. 113. (Brazil, 2024).

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056EN
2025 | v. 19 | n. 3 | p. 1-24 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056EN

attacks) with inaccuracy can lead to generalizations that do not favor the application of the law, quite the contrary.

Regarding the debate on the application of Article 43 of the LGPD, the vote continues, establishing that "a data leak will not always be recognized as an external fortuitous event, therefore, capable of eliminating the civil liability of the agent," and that it may be considered an internal fortuitous event, which is even compared to the provision of statement No. 479 of the STJ Summary, which provides that financial institutions are objectively liable for damages caused by internal fortuitous events related to fraud and crimes committed by third parties in the context of banking operations (Brazil, 2024). For an internal fortuitous event to be established, it would be necessary that *(i)* the data leak was an inherent risk of the activity or *(ii)* that the organization's lack of preparation was a determining factor in the occurrence of the incident.

This point, and even the analogy to the STJ's summary statement, is promising and could well be used in other cases, such as those involving damage resulting from cyber attacks. However, the obvious caveat applies: in addition to further theoretical study of this possibility, the classification of an internal fortuitous event involving a cyber attack may depend greatly on the circumstances in which the attack occurred, as well as the method of attack used, the security measures adopted (or not), the conduct of the victim, among other aspects of the specific case.

Furthermore, the decision states that the processing of data became irregular when it failed to provide security to the data subject ("expectation of legitimate protection"), pursuant to Article 44, item III, of the LGPD[10]. By failing to prove, before the lower courts, that the leak of the respondent's data occurred exclusively as a result of the security incident, it would be impossible to apply the exclusion of liability under Article 43, III, of the LGPD in favor of the appellant Eletropaulo - even due to the legislative technique, which imposes on the processing agent the burden of proving the breach of the causal link. For this reason, it is certain that the processing agent will be liable for violations resulting from a breach of the duty of security, especially when it fails to adopt the technical and administrative measures set forth in the legal text, notably against "unauthorized access (security incidents and hacker attacks), and

10 Art. 44. The processing of personal data shall be unlawful when it fails to comply with the law or when it does not provide the security that the data subject can expect, considering the relevant circumstances, including: [...] III - the techniques for processing personal data available at the time it was carried out.

accidental or unlawful situations of destruction, loss, alteration, communication, or any form of inappropriate or unlawful processing." (Brazil, 2024).

Therefore, the Superior Court ruled against the arguments put forward by the appellant Eletropaulo, since *(a)* even if the leak had resulted from an "unlawful security incident," there was no evidence in the case file that the appellant had adopted the security measures established in the LGPD, which could be necessary and sufficient for the protection of the data subject's data, and *(b)* there is no way to attribute exclusive fault to a third party in the absence of evidence that the data leak occurred strictly as a result of the cyber attack. The precedent highlights the need for compliance with the duty of security in the operations and activities of personal data processing by processing agents (meeting the security expectations of data subjects), in addition to the fact that negligence and insufficient protection (even in the context of cyber attacks) may characterize an internal fortuitous event, giving rise to civil liability for those involved.

3.2 The case AREsp n° 2.130.619-SP

The case in question, judged by the STJ in Special Appeal (AREsp) No. 2.130.619-SP, refers to a lawsuit for moral damages filed by a private individual against the electricity concessionaire Eletropaulo Metropolitana Eletricidade de São Paulo S.A. (now ENEL). The cause of action is a security incident involving the leakage and access, by third parties unrelated to the commercial relationship, of the customer's personal and contractual data. The leaked data included information such as full name, ID number, gender, date of birth, age, landline telephone number, cell phone number, address, as well as data related to the electricity supply contract (installed load, estimated consumption, type of installation, and consumption readings). The plaintiff claimed that the exposure of this information put her at potential risk of fraud and harassment, and in view of the unlawful act, she sought compensation for moral damages (Brazil, 2023b).

The claim was dismissed in the first instance on the grounds that the leaked data was common, not covered by confidentiality, and that knowledge by third parties did not violate the plaintiff's personality rights, as there was no effective proof of damage, an essential requirement for establishing the duty to compensate. The São Paulo State Court of Justice overturned the ruling and ordered the utility company to pay compensation, basing its decision, among other reasons, on the fact that the data was the personal data of an elderly person and considering that the leak of confidential data

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056EN
2025 | v. 19 | n. 3 | p. 1-24 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056EN

constituted a failure in the provision of services. In this case, the TJSP ruling classified the leaked data as sensitive (Brazil, 2023b).

When analyzing the utility company's appeal, STJ addressed procedural issues, such as the absence of a preliminary question regarding the thesis of exclusive third-party liability but focused its decision on the legal matter related to data leakage from the perspective of the LGPD. The Superior Court accepted the concessionaire's argument regarding the classification of data, highlighting that Article 5, II, of the LGPD provides an exhaustive list of sensitive personal data that requires special treatment. The data leaked in this specific case included names, ID numbers, telephone numbers, and addresses, which are characterized as personal data but do not fall under the legal classification of sensitive data (Brazil, 2023b).

The crucial point of the STJ's decision, therefore, lies in the legal treatment given to moral damage resulting from the leakage of common personal data. The court established that the leakage of personal data does not have the power to generate compensable moral damages. In order to be entitled to compensation, the data subject must prove the actual damage resulting from the exposure of the information. The STJ differentiated this situation from the leakage of sensitive data, which concerns the privacy of natural people, suggesting that the legal consequences could be different in such cases. Thus, with the granting of the concessionaire's special appeal, the dismissal of the claim for compensation for moral damages was reinstated (Brazil, 2023b).

Although legally based on the requirements of civil liability and the interpretation of the LGPD provision, the decision can be criticized regarding its assessment of the triggering event as a security incident and the repercussions of this approach. In analyzing the case, the STJ correctly identified the event as a "leak and access by third parties" to the plaintiff's personal and contractual data. The court recognized that this was an "undesirable failure in the processing of natural person data by a legal entity" (Brazil, 2023b). This recognition is in line with the definition of a personal data security incident, understood as any adverse and confirmed event related to a breach in personal data security, including unauthorized access or leakage, which jeopardizes the rights of data subjects. The leak itself is characterized by the obtaining and exposure of data.

However, criticism arises from the legal consequences attributed to this incident, for underestimating the risk and potential damage inherent in the leakage of common data, even if the damage does not immediately materialize in a way that is

easily verifiable by the victim or if the data is sensitive. Sources that deal with security incidents point out that the leakage of personal data, being a critical type of incident, favors criminals with the opportunity to commit various types of crimes such as fraud, obtaining passwords, cloning credit cards, and allows the use of social engineering to deceive and take advantage of citizens. The damage to citizens is therefore directly related to the opportunity that this leak provides, without the need to prove actual damage.

By requiring proof of actual damage for common data, the STJ's decision seems to focus more on traditional civil liability, which has proof of damage as an essential element, than on the severity of the security incident itself and the risk it creates for the data subject. The exposure of information such as name, ID number, telephone number, and address, although common, are precisely the building blocks for many fraudulent activities—which can even be enhanced by the malicious use of technology, such as artificial intelligence systems, deep fakes, among others. The plaintiff in the case claimed precisely the potential danger of fraud and harassment, which, in the view of the STJ, was not sufficient without proof of actual damage (Brazil, 2023b).

The importance of reporting security incidents, as highlighted initially, lies in the detection, prevention, and containment of damage and losses, and in compliance with regulatory obligations, which ultimately aim to protect data subjects and allow the ANPD to assess the severity and the measures taken. The mere occurrence of the leak already imposes obligations on the controller and generates the need for mitigation actions. The STJ's decision, by requiring proof of damage for the purposes of compensation for moral damages in common data leaks, places a considerable burden on the data subject, who may have difficulty tracking and proving that a specific damage, such as an attempt at fraud or harassment, resulted directly from that particular leak, especially if the leak is extensive and their data is used in conjunction with other sources (Brazil, 2023b).

In short, while the STJ's decision is in line with the need to prove moral damages in cases that do not involve sensitive data, it could be criticized for potentially minimizing the consequences of the security incident itself, focusing only on the material damage and not on the significant risk created by the unauthorized exposure of personal data, even if common. This approach may send a message that incidents involving common data are of less legal relevance to the data subject, despite the potential for malicious use highlighted in sources on digital security.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056EN
2025 | v. 19 | n. 3 | p. 1-24 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056EN

4. Conclusions

S In the digital age, characterized by the exponential expansion of data circulation and growing dependence on information systems, society is increasingly vulnerable to security incidents, notably cyber attacks and data leaks, which, far from being mere technical setbacks, pose concrete and multifaceted threats to legal protection and fundamental rights, such as privacy and the protection of personal data. Thus, the growing sophistication of digital threats and the multiplicity of forms, agents, and impacts that these incidents can pose significant challenges for the application of the law, requiring normative and jurisprudential responses that are commensurate with their technical complexity and the systemic risks involved.

An analysis of the precedents of the Superior Court of Justice, in particular REsp 2.147.374/SP and AREsp 2.130.619/SP, reveals nuances and partially divergent responses regarding the civil liability of data processing agents. The first ruling points to objective and proactive liability, emphasizing the duty of the agent to adopt adequate security measures, even if the incident results from unlawful conduct by a third party, and recognizing the expectation of legitimate protection on the part of the data subject. The second, in turn, when dealing with the leakage of non-sensitive data, aligns itself with the traditional logic of subjective civil liability, reinforcing the need to prove actual damage for compensation purposes.

The application of the law by the STJ in view of the complexity and multiple nuances of security incidents, such as leaks and cyber attacks, has been partially divergent. There is a transition between two models of liability: one that points to the objective and proactive liability of the processing agent, emphasizing the duty of adequate security; and another that aligns with traditional subjective logic, requiring proof of actual damage for compensation purposes in cases of leakage of non-sensitive personal data. This dissent and the possible conceptual generalization of the term "security incidents" are critical, as they tend to underestimate the risk and potential damage inherent in the mere improper exposure of information, imposing a considerable burden on the data subject and compromising the effective protection provided for by standards such as the LGPD, the MCI, and the CDC.

The interpretative dissent and possible generalization of the term "security incidents" in legal discourse highlight the premise of greater conceptual and technical accuracy in the classification of these events. An indistinct approach to the causes,

nature, and effects of incidents tends to compromise the effectiveness of the protection afforded by the LGPD and the legal certainty of decisions themselves. At this point, the requirement to prove damage in cases of data leaks considered "common" is criticized, as it underestimates the risk and potential damage inherent in the mere improper exposure of personal information. Leaks of personal data, even those not classified as sensitive, facilitate crimes such as fraud, scams, and misuse, placing data subjects at real risk. Requiring the data subject to prove the causal link between the leak and specific damage imposes a considerable burden and may constitute an obstacle to the realization of the fundamental right to data protection.

Given this scenario, it is necessary to consolidate an interpretative framework that, consistent with the provisions of the LGPD, recognizes the inherent seriousness of security incidents. An improved understanding of nature and consequences of these events, dissociated from simplistic generalization, must take into account the classification and risk they represent, regardless of the specific nature of the data exposed. Any civil liability must, therefore, weigh more robustly the failure to adopt preventive measures and the mere exposure of data subjects to concrete risks, even in the absence of immediately quantifiable damages. A focus on the measures adopted to contain, manage, and stabilize the damage caused by the incident, combined with the recognition of risk as a relevant element of liability, will ensure more effective protection of fundamental rights in the digital environment and foster the culture of information security advocated by the legislation.

REFERENCES

ANPD. *Atividades Fiscalizatórias.* Avaliable at: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos?_authenticator=b05dbbec15247ce4c8b7065d588ef945f6d4d340. Access on: 16 Apr. 2025.

ANPD. *Incidentes de segurança com dados pessoais*. 2022. Avaliable at: https://www.gov.br/anpd/pt-br/acesso-a-informacao/acoes-e-programas/programas-projetos-acoes-obras-e-atividades/semana-da-protecao-de-dados-2022/incidentes-de-seguranca-com-dados-pessoais. Access on: 14 Mar. 2025.

ANPD. *Resolução CD/ANPD nº 15, de 24 de abril de 2024.* Aprova o Regulamento de Comunicação de Incidente de Segurança. Avaliable at: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Access on: 11 Dec. 2025.

BRANQUINHO, T.; BRANQUINHO, M. *Segurança cibernética industrial.* Rio de Janeiro: Alta Books, 2021.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056EN
2025 | v. 19 | n. 3 | p. 1-24 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056EN

BRASIL. *Decreto nº 10.222, de 5 de fevereiro de 2020*. Aprova a Estratégia Nacional de Segurança Cibernética. 2020a. Avaliable at: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Access on: 20 Feb. 2025.

BRASIL. *Decreto nº 10.569, de 9 de dezembro de 2020*. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. 2020b. Avaliable at: https://www.planalto.gov.br/cCivil_03/_Ato2019-2022/2020/Decreto/D10569.htm. Access on: 20 Feb. 2025.

BRASIL. *Decreto nº 11.856, de 26 de dezembro de 2023.* Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. 2023a. Avaliable at: https://www.in.gov.br/en/web/dou/-/decreto-n-11.856-de-26-de-dezembro-de-2023-533845289. Access on: 20 Feb. 2025.

BRASIL. Superior Tribunal da Justiça. STJ. *AREsp n. 2.130.619/SPb*. 2023b. Relator Ministro Francisco Falcão, Segunda Turma, julgado em 7/3/2023, DJe de 10/3/2023.

BRASIL. Superior Tribunal de Justiça. STJ. *Recurso Especial n. 2.147.374/SP*. Relator Ministro Ricardo Villas Bôas Cueva, Terceira Turma, julgado em 3/12/2024, DJEN de 6/12/2024.

CARVALHO, A. C.; SOUZA, V. L. e. Segurança da informação e resposta a incidentes de vazamento no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD). *Revista do Advogado*, n. 144, nov. 2019.

CERT.br; NIC.br; CGI.br; ANPD. *Vazamento de dados*. Avaliable at: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf. Access on: 13 Mar. 2025.

CISCO. *What is a cyberattack?* Avaliable at: https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-cyberattack.html. [*s. d.*]. Access on: 15 Jan. 2025.

FREIRE, A. *et al.* (org.). *Jornada segurança da informação*: unindo visão executiva e técnica para estratégia, comportamento, inovação e tendências. Rio de Janeiro: Brasport, 2024. *E-book*. Avaliable at: https://plataforma.bvirtual.com.br. Access on: 2 Sep. 2025.

HINTZBERGEN, J. *et al. Fundamentos da segurança da informação*: com base na ISO 27001 e na ISO 27002. Tradução: Alan de Sá. Rio de Janeiro: Brasport, 2018.

JIMENE, C. do V. Capítulo VII: da segurança e boas práticas. *In*: MALDONADO, V. N.; OPICE, B. R. (coord.). *LGPD*: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019. *E-book*.

LUCIANO, M. Vazamentos de dados na LGPD: em busca do significado de "incidentes de segurança". *Revista do Advogado*, n. 144, nov. 2019.

OLIVEIRA, A. G. de; GOMES, T. R. P. de A.; MATTEU, I. F. de. Vazamento de dados e dano moral: uma análise a respeito do entendimento de julgados do Tribunal de Justiça de São Paulo. *Revista de Direito Constitucional e Internacional*, v. 139, p. 11-25, set./out. 2023.

PARLAMENTO EUROPEU. Regulamento (EU) 2024/2847 do Parlamento Europeu de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.º 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828 (Regulamento de Ciber-Resiliência). *Jornal Oficial da União Europeia*, 20 nov. 2024. Avaliable at: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L_202402847. Access on: 24 Aug. 2025.

PETRY, G. C.; HUPFFER, H. M. O princípio da segurança na era dos ciberataques: uma análise a partir do escopo protetivo da LGPD. *Revista do CNJ*, v. 7, n. 1, 2023.

QUEIROZ, J. Q.; MORAES, M. C. B. de. Autodeterminação informativa e responsabilização proativa. *Cadernos Adenauer*, v. XX, n. 3, p. 113, 2019.

SCHNEIER, B. *Click here to kill everybody*: security and survival in a hyper-connected world. New York: W.W. Norton & Company, 2019.

SILVA, M. B. F. da. *Cibersegurança*: [...]. Rio de Janeiro: Freitas Bastos, 2023.

Gabriel Cemin Petry

Master's student in Public Law at Unisinos, with a PROEX/Capes scholarship. Holds a Bachelor's degree in Law from Feevale University. Member of the CNPq/Feevale Research Group: Law and Development. Member of the CNPq/Feevale Research Project: Artificial Intelligence for a Sustainable Future: Legal and Ethical Challenges; member of the Jusnano/CNPq Research Group; collaborator at the Mediterranea International Centre for Human Rights Research (MICHR), Italy. Lawyer. Author of legal articles.
Universidade do Vale do Rio dos Sinos
Novo Hamburgo, RS, Brasil
E-mail: Gabrielcpetry96@gmail.com

Karin Regina Rick Rosa

Lawyer. Master's Degree in Law from Unisinos University. Specialist in Civil Procedural Law. Professor of Civil Law and Notarial and Registry Law. Member of the Brazilian Notarial Academy – Chair No. 38. Member of the Executive Board of IBDFAM-RS. Member of the Advisory Council of IBRADIM. Holds international EXIN certifications in Data Protection and Privacy, and Information Security Systems. Book coordinator and author of legal articles.
Universidade do Vale do Rio dos Sinos
Novo Hamburgo, RS, Brasil
E-mail: karinrick.rosa@gmail.com

Wilson Engelmann

Ph.D. and Master in Public Law from the Graduate Program in Law at Universidade do Vale do Rio dos Sinos (Unisinos), Brazil. Completed a Postdoctoral Fellowship in Public Law and Human Rights at the Centro de Estudios de Seguridad (CESEG), University of Santiago de Compostela, Spain. Professor and Researcher in the Graduate Program in Law (Master's and Doctorate) and in the Professional Master's Program in Business and Corporate Law, both at Unisinos. CNPq Research Productivity Fellow. Leader of the JUSNANO Research Group, accredited by CNPq.
Universidade do Vale do Rio dos Sinos
Novo Hamburgo, RS, Brasil
E-mail: wengelmann@unisinos.br

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056EN
2025 | v. 19 | n. 3 | p. 1-24 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056EN