RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

Between Privacy and Cybercrime: Criminal Law Inadequacy in the Data Age

Between Privacy and Cybercrime: Criminal Law Inadequacy in the Data Age

Kelly Beatriz Sousa do Nascimento
Khayam Ramalho da Silva Sousa

SUMMARY

The exponential expansion of digital technologies, while reshaping social and economic dynamics, catalyzes the proliferation of cybercrimes, posing critical challenges to the traditional penal system. This article investigates the extent to which the General Data Protection Law (Law No. 13.709/2018) operates as a strategic instrument in the prevention and repression of digital criminal conduct and identifies the main obstacles to its application in the penal sphere, notably in the classification, investigation, and sanctioning of offenses. Methodologically, the study is based on a narrative and doctrinal bibliographic review, consulting specialized scientific databases such as SciELO and Google Scholar. The results show that, although the LGPD constitutes an essential normative advance for the protection of privacy, its contribution to penal repression is severely limited by the absence of specific classifications in the Penal Code and by the transnational complexity of virtual environments. It is concluded that the criminal protection of personal data requires systemic reform, demanding the development of more robust legal instruments, massive investment in institutional capacity building for legal professionals, and the urgent strengthening of international legal cooperation for the effective fight against cybercrime.

Keywords: LGPD (Brazilian General Data Protection Law). Cybercrimes. Digital Criminal Law. Digital Privacy.

ABSTRACT

The exponential expansion of digital technologies, while reconfiguring social and economic dynamics, catalyzes the proliferation of cybercrime, imposing critical challenges to the traditional penal system. This article investigates to what extent the General Personal Data Protection Law (Law No. 13,709/2018) operates as a strategic instrument in preventing and repressing digital criminal conduct and identifies the main obstacles to its application in the criminal sphere, notably in the typification, investigation, and sanctioning of crimes.

Methodologically, the study is based on a narrative and doctrinal bibliographic review, consulting specialized scientific databases such as SciELO and Google Scholar. The results show that, although the LGPD constitutes an essential normative advance for privacy protection, its contribution to criminal repression is severely limited by the absence of specific typifications in the Penal Code and the transnational complexity of virtual environments. It is concluded that the criminal protection of personal data requires a systemic reform, demanding the development of more robust legal instruments, massive investment in institutional capacity-building for legal operators, and the urgent strengthening of international legal cooperation to effectively combat cybercrime.

Keywords: LGPD. Cybercrime. Digital Criminal Law. Digital Privacy.

1. Introduction

The advancement of digital technologies, coupled with the growing dependence on interactions Mediated by the internet, it has brought numerous benefits to contemporary society, but also This has given rise to new and sophisticated forms of crime. Cybercrimes, characterized by conduct that uses computer systems as an illicit means or end,

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

They present exponential challenges for criminal law, especially with regard to the protection of privacy and security of personal data. In this context, the enactment of the General Data Protection Law The Personal Data Protection Law (Law No. 13.709/2018) represented an essential regulatory milestone. in Brazil, seeking to align the national legal system with international trends of protection of privacy (Silva; Novais, 2023).

The LGPD (Brazilian General Data Protection Law) emerged as a response to the need to regulate the collection and storage of data. and the use of personal information in digital environments, aiming to guarantee greater control on the part of data subjects. However, this very centrality of personal data has transformed them into a primary target for criminals, who exploit technological vulnerabilities to commit crimes. illicit conduct. The increased incidence of electronic fraud, system intrusions and Leaks of sensitive information expose the fragility of security measures, revealing a gap. criticism between data protection legislation and the effective capacity of criminal law in to suppress these practices (Damião; Novais, 2024).

This type of digital crime is characterized by its technical complexity and... The transnational nature of the conduct imposes significant obstacles to investigation and prosecution. criminal prosecution. The very definition of many crimes still does not keep pace with the dizzying pace of crime. Technological evolution has led to situations where the application of the Brazilian Penal Code is necessary. shows insufficient to adequately frame certain illicit practices (Zechariah; Freire, 2023).

Therefore, such dissonance raises urgent questions about the need for creation of new specific criminal offenses, capable of providing greater legal certainty and effectiveness in combating digital offenses. The protection of personal data, elevated to the status of fundamental right, reinforces the importance of a penal approach that is compatible with The guidelines of the LGPD (Brazilian General Data Protection Law) are followed, but practical implementation difficulties are faced, both in the sphere... administrative (ANPD) as well as in the criminal sphere.

Given this scenario, this article seeks to answer the following question: Research: To what extent does the General Data Protection Law (LGPD) contribute to the Prevention and repression of cybercrimes, and what are the main challenges in this regard? application in the criminal field, especially in the classification, investigation and punishment of conduct. criminals?

Therefore, the study's general objective is to critically analyze the interrelationship between The LGPD (Brazilian General Data Protection Law) and Brazilian Criminal Law, identifying normative potential and limitations. of repressive action. Methodologically, a literature review will be employed and documentary, based on scientific literature, legislation and official documents (Duarte, 2022;

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

Costa; Silva, 2022).

The aim is, therefore, to contribute to the academic and legal debate by defining the...
Possibilities for the LGPD (Brazilian General Data Protection Law) to act as a tool in combating crime.
Digital technology in Brazil. The article is structured in four sections, which will successively address the...
Fundamentals of data protection and cybercrime, the LGPD (Brazilian General Data Protection Law) and its relationship with...
Criminal Law, the challenges in investigating and punishing cybercrimes, and finally, the
Proposals and perspectives for the criminal protection of personal data.

2. Fundamentals of data protection and cybercrime, and the evolution of legislation in Brazil

The protection of personal data in Brazil is the result of a gradual legislative process, which
This reflects the need to keep pace with rapid technological evolution and increasing digitalization.
of social relations.

Initially, the topic was addressed in a diffuse manner by the 1988 Federal Constitution, which
It guaranteed rights to privacy, intimacy, honor, and confidentiality of communications, but not
It directly addressed data protection as an autonomous category. The absence of a
Specific legislation focused on the digital environment left gaps that were filled by regulations.
scattered, hindering the effectiveness of defending privacy and suppressing illegal conduct.
This scenario began to change with the strengthening of the debate on digital rights in
2000s, driven by the increased use of the internet in the country (Silva; Novais,
2023).

In this context, the Brazilian Internet Bill of Rights (Law No. 12.965/2014) emerged as the first...
A major Brazilian regulatory milestone focused on regulating the virtual environment. The law established
fundamental principles, such as guaranteeing net neutrality, protecting privacy, and...
responsibility of service providers. Although it did not have protection as its central focus.
Regarding personal data, the Civil Rights Framework for the Internet represented a considerable step forward, as it enshrined the...
User privacy as a fundamental right in the digital environment. Furthermore,
It established rules for the storage and provision of connection and access logs, creating
minimum legal security parameters for the use of the network (Zacarias; Freire, 2023).

With the Civil Rights Framework for the Internet, space was opened for discussion about the need for a
specific law for the processing of personal data. This intensified in light of...
global transformations in the field of data protection, especially after the enactment of
The European Union's General Data Protection Regulation (GDPR), in 2016, which inspired

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

several countries are updating their domestic legislation.

In this sense, Brazil, situated within a globalized and interconnected world, needed adapt its legal system to maintain trade relations with countries that already required stricter protection standards, such as those of members of the European Union. This external factor was... crucial for accelerating the development of a national regulatory framework specifically aimed at... to data protection (Souza *et* al., 2024).

Indeed, the enactment of the General Law on the Protection of Personal Data (Law No. Law 13.709/2018 thus constituted a watershed moment. The LGPD (Brazilian General Data Protection Law) provided detailed regulations. the collection, processing, storage, and sharing of personal data, bringing Concepts such as controller, operator, data subject, and legal bases for processing. The law It also reinforced principles such as transparency, purpose, necessity, and security, seeking To balance the economic use of information with the preservation of human dignity. Its The approval marked Brazil's entry into a new level of regulatory protection, aligning- already established international standards (Silva; Novais, 2023).

Furthermore, another important aspect of the LGPD was the creation of the National Data Protection Authority. Data Protection Authority (ANPD), responsible for overseeing and applying administrative sanctions in Cases of non-compliance. This institutionalization was essential to ensure the effectiveness of the law. because one of the major problems with the previous regulations was the lack of specialized bodies. capable of overseeing compliance with the rules.

With the ANPD (National Data Protection Authority), the legislation gained concrete *enforcement mechanisms,* even though... limited to the administrative field, which highlights the need for integration between the tutelage civil, administrative, and criminal law in addressing violations related to personal data. (Damião; Novais, 2024).

However, despite its advancements, the LGPD's main characteristic is its nature. administrative, failing to provide specific criminal offenses for conduct related to misconduct. use of personal data. This absence generates debate in legal doctrine, because even though the Penal Code While it may include crimes such as computer intrusion and breach of confidentiality, there are practices... modern criminal activities, such as mass data leaks or the illicit sale of... Sensitive information that does not fit into any specific legal definition under current criminal law.

In this way, the LGPD contributes to prevention and accountability. administrative, but reveals limitations when it comes to the criminal prosecution of cybercrimes. (Zacarias; Freire, 2023).

Furthermore, regulatory evolution in Brazil did not occur in a linear fashion, but as Response to social demands and international pressure. Emblematic cases of leaks of

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

Data breaches, electronic fraud, and hacker attacks have had media and political repercussions.
pressuring the legislature to move forward in creating specific regulations. This trajectory demonstrates
Brazilian legislation on data protection is reactive rather than preventive.
This reinforces the importance of research that critically analyzes the effectiveness of laws.
existing ones and point out the need for improvements (Costa; Silva, 2022).

the effort to adapt the legal system to the new dynamics of society.
information. However, this process is far from complete: there are still regulatory gaps,

Reviewing this historical trajectory is essential to understanding current limitations and possible paths forward.
possible ways to strengthen the criminal protection of personal data in the country, thus guaranteeing,
greater legal certainty in an increasingly vulnerable digital environment (Duarte, 2022;
Souza et al., 2024).

Therefore, it is clear that the consolidation of an effective legal system for the protection of
Data depends not only on new laws, but also on a paradigm shift regarding...
Information culture in Brazil. Legislation must be accompanied by public policies of
Raising awareness, training public officials, and expanding cooperation mechanisms.
international. Only from this combination of regulations, digital education and
Effective criminal prosecution will make it possible to ensure the effective protection of fundamental rights.
Citizens in the digital age.

2.1 The right to the protection of personal data as a fundamental right

The recognition of personal data protection as a fundamental right represents
A significant achievement in strengthening the democratic rule of law in Brazil.
The 1988 Federal Constitution already guaranteed, in its article 5, the inviolability of privacy.
of private life and the confidentiality of communications, but did not foresee the protection of data such as
autonomous category. With the advancement of digital technologies and the increasing circulation of
information made it clear that a specific right aimed at protecting the need for a specific right became evident.
Informational privacy, since personal data has become an instrument
of political and economic power (Silva; Novais, 2023).

This recognition gained strength with Constitutional Amendment No. 115/2022, which
It expressly included the protection of personal data in the list of fundamental rights and guarantees.
equating it to values such as freedom and dignity. According to Souza *et al.* (2024), such a measure

RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

"It reconfigures the role of the State, imposing on it the duty to ensure the integrity of..." "Personal information as an extension of human personality." Thus, data protection It is no longer a topic restricted to public administration and has become part of the sphere of rights. fundamental, directly linking the State and private enterprise to the duty of guaranteeing Information security.

The constitutionalization of this right has brought important practical implications, especially in the field of public policies and legal sanctions. As highlighted by Damião and Novais (2024), that the violation of personal data must be treated as an attack on human dignity, demanding a response proportional to the severity of the damage. This interpretation reinforces the The need for more effective legal mechanisms, including criminal ones, to deal with conduct. who use technology as a means of violating rights.

In this context, the principle of informational self-determination stands out, enshrined in European doctrine, incorporated by the LGPD (Brazilian General Data Protection Law), consolidates the understanding that each An individual has the right to control the use and circulation of their information. As explained According to Duarte (2022), the data subject must have decision-making power over their own data, which represents a new dimension of individual freedom and human dignity. In Brazil, the internalization This principle, as enshrined in the LGPD (Brazilian General Data Protection Law), reinforces the view that privacy extends beyond the field. patrimonial and reaches the essential core of personality.

In addition to guaranteeing individual autonomy, data protection has a collective character. and social. Therefore, massive leaks, fraud, and cyberattacks demonstrate that the Improper handling of information can compromise not only the security of a citizen, but public trust in institutions. In this perspective, Costa e Silva (2022) They emphasize that criminal law protecting data is necessary not only to punish misconduct. individual, but also to preserve the stability of digital and economic relationships that They support contemporary society.

In the international arena, the constitutionalization of data protection reinforces the Brazil's integration into global information security standards, facilitating agreements of Cooperation in the fight against cybercrime. Countries with compatible legislation tend to collaborate. more efficiently in the investigation and repression of digital crimes, which positions Brazil as a relevant actor in this emerging legal field (Souza *et al.,* 2024).

Despite the progress, the realization of this right depends on its effectiveness. application. Constitutional recognition, by itself, does not guarantee real protection if there is no public policies on information security, investments in technological infrastructure and Capacity building for oversight and investigative bodies. The lack of integration between the spheres.

RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

Administrative, civil, and criminal law remains an obstacle to the consolidation of comprehensive data protection. personal (Zacarias; Freire, 2023).

Therefore, it is possible to state that data protection as a fundamental right does not It should be seen not only as a legislative innovation, but as an ethical commitment and Politics, freedom, and human dignity are essential. Brazil needs to move beyond mere formality. regulations for practical effectiveness, promoting a culture of digital responsibility and Strengthening the role of the State and institutions in guaranteeing informational privacy. Only through this integration will it be possible to consolidate a full and adapted legal protection. to the complexities of the digital age.

3. The intersection between the LGPD and the provisions of the Brazilian Penal Code

The intersection between the General Data Protection Law (Law No. 13.709/2018) and the The Brazilian Penal Code represents a milestone in the evolution of the national legal system in combating digital crimes. The LGPD, although predominantly in nature administrative and civil law introduces principles and obligations that directly impact the sphere. penal law, serving as an interpretative parameter for the repression of conduct involving the unlawful processing of personal data.

In this sense, Silva and Novais (2023, p. 9) highlight that “the LGPD does not create criminal offenses, but it guides the application of contemporary criminal law, especially in contexts of "Violation of informational privacy and misuse of sensitive data."

The Penal Code, in turn, includes provisions that touch upon the protection of intimacy and private life, such as the crimes of violation of correspondence (art. 151), Disclosure of secrets (article 153) and falsification of documents (article 299). However, the rapid Digital transformation has exposed the inadequacy of these traditional norms to encompass new realities. Forms of technological delinquency. Including, with the enactment of Law No. 12.737/2012, Known as the Carolina Dieckmann Law, it represented progress by criminalizing the invasion of computer devices.

At this point, it is worth highlighting the points made by Zacarias and Freire (2023, p. 36), that “the Brazilian criminal laws remain fragmented, lacking systematic updating to "To keep up with the complexities of cyberspace and the sophistication of information attacks." Thus, the LGPD emerges as a complementary instrument of preventive criminal policy. imposing on individuals and legal entities the duty to adopt technical and security measures. organizational. Deliberate failure to comply with these obligations may constitute illegal acts.

RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

criminal offenses, such as violation of professional secrecy (article 154 of the Penal Code) or theft.
qualified by means of electronic fraud (art. 155, §4º-B).

Thus, Dias (2021, p. 46) states that:

> Organizations need to adapt to the General Data Protection Law (LGPD), since irregular data sharing or data breaches, even accidentally, will subject them to various penalties, both under the aforementioned law and other applicable regulations. Therefore, companies that collect and store this information must implement the LGPD through a series of measures contained within it, aiming to prevent the irregular sharing of these knowledge bases and review their information security policies, adapting them to the specificities of sensitive personal data or data of children and adolescents, respecting the principles of the LGPD. It is inconceivable to view the protection of this content as a mere costly act, instead of a necessary investment capable of conveying to the data subject the concern of the data controllers for their privacy and security. Therefore, administrative sanctions, liability, and compensation for damages arising from lack of information security and irregular data sharing are instruments added by the Brazilian legislator through national legislation and the LGPD (Brazilian General Data Protection Law), with the aim of encouraging a culture of ethics based from the outset on current regulations, ensuring that service providers are aware of the choices from the outset that integrate privacy and other ethical principles in products and services that handle these personal elements.

Beyond the material aspect, the LGPD influences the procedural dimension of criminal law.
establishing guidelines for the collection, storage, and use of digital evidence. The principle of
The principle of proportionality, implicitly foreseen in the text of the law, requires that the processing of data in
Criminal investigations must respect legitimate purposes and the right to privacy. (Souza *et al.)*
(2024) emphasize that the abusive use of data without a legal basis can lead to procedural nullities.
and state accountability, reinforcing the role of the LGPD as an instrument for controlling
punitive power.

However, another point of convergence lies in the definition of sensitive personal data.
category introduced by the LGPD to define information that requires greater protection, such as
Religious beliefs, genetic and biometric data. The criminal manipulation of this data.
This can aggravate the penalty, since the potential for moral and social harm is significantly greater.
high. Costa and Silva (2022) argue that the use of such data in fraudulent practices
It should be understood as an injury to human dignity, and not merely as a financial offense.

The interface between the General Data Protection Law and the Penal Code reveals
complex challenges of an interpretative and dogmatic nature, especially with regard to
The necessary harmonization between the principles of minimum intervention and proportionality is required.
criminal law and the state's duty to ensure effective and comprehensive protection of privacy and rights.
of personal data. Such reconciliation requires a systematic reading that preserves consistency.
of the legal system, preventing the undue expansion of criminal law into spheres already...

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

sufficiently regulated by administrative and civil sanctioning law. Duarte (2022) highlights that the objective is to avoid "penal expansionism" and ensure that the criminalization of conduct Regarding issues related to the improper handling of data, this should only occur when it is indispensable for protection. of fundamental legal rights.

Despite structural limitations, the LGPD has promoted important advances in Accountability of agents who commit digital crimes. The obligation to report. of security incidents, for example, it creates transparency mechanisms that facilitate the The role of bodies such as the Public Prosecutor's Office and the National Data Protection Authority. (ANPD). Cooperation between these institutions is essential to strengthen criminal prosecution and to reduce impunity in cases of leaks or illegal sale of information. personal (Silva; Novais, 2023; Souza *et al.,* 2024).

Furthermore, the practical application of the LGPD (Brazilian General Data Protection Law) in the criminal sphere depends on an integrated approach between justice institutions and civil society. It is necessary that prosecutors, Delegates and digital experts understand the technical and ethical foundations of the law, so that to ensure the proper investigation of cybercrimes. This interdisciplinary approach is crucial so that legislation should achieve its social purpose and not be restricted to the letter of the law.

In short, the convergence between the LGPD (Brazilian General Data Protection Law) and the Penal Code reflects the State's efforts. Brazilian citizens are updating their criminal policy in the face of the challenges posed by the digital age. More Rather than establishing new types of crimes, it is about promoting a legal culture geared towards... prevention and proportional accountability. The consolidation of this intersection depends on legislative reforms that provide greater precision to information crimes, but also of A cultural shift that values ethical data use and digital literacy among the population.

Thus, the protection of personal data ceases to be a mere administrative guideline and becomes... to affirm itself as a true pillar of the Democratic Rule of Law, capable of balancing Freedom, security, and responsibility in a connected society.

4. Cybercrimes and the role of the LGPD in prevention and combating them.

The discussion about the need to create new criminal offenses related to The protection of personal data and the fight against cybercrime have gained increasing relevance in contemporary legal scenario. Although the General Law on the Protection of Personal Data (Law No. Law 13.709/2018) has represented a substantial advance in the administrative and civil regulation of Regarding the handling of information, it did not establish its own penal mechanisms for To hold accountable those responsible for conduct that causes serious harm to informational privacy.

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

Well, according to Silva and Novais (2023), this gap highlights the challenge of adapting the criminal law in a constantly transforming technological context, where new forms of Crime emerges in a dynamic and transnational way.

The Brazilian Penal Code, created in 1940, was conceived within a historical context. completely different, in which social and economic relations did not depend on means digital. Despite specific reforms, such as the introduction of article 154-A by Law No. 12.737/2012 (Carolina Dieckmann Law) and electronic fraud by Law No. 14.155/2021, the The criminal justice system still does not adequately address the complexity of cybercrimes. Zacarias and Freire (2023, p. 22) state that:

> Brazilian criminal law, while advancing in the criminalization of device intrusion and the protection of computer systems, remains insufficient to meet the demands of the information society, leaving uncovered various behaviors that violate the fundamental right to privacy.

In fact, new forms of digital attack, such as *ransomware and phishing,* are emerging. advanced algorithmic manipulation, virtual identity cloning, and massive data leaks. Data transcends the limits of traditional criminal offenses. The LGPD, although it brings principles and obligations, it lacks repressive mechanisms that guarantee proportionate responses to such violations. Damião and Novais (2024, p. 11) emphasize that “the absence of specific criminal offenses that address the willful violation of personal data weakens the protection system and compromises "The effectiveness of public policies on information security."

Thus, the need for regulatory updates does not imply mere expansionism. penal, but the adaptation of punitive norms to the new digital reality. Including, as well as highlighted by Almeida (2015, pp. 222-223), who states that:

> Proportionate to the benefits that have arisen with the internet, there have also been illicit activities carried out by agents specializing in this field. Such behaviors are known by various names, such as cybercrimes, cybercrimes, and other criminal activities. Cybercrimes, digital crimes, computer crimes, telematics, high-tech crimes, computer crimes, internet crimes, computer fraud, transnational crimes, among others. Within this context, we have the figure of the cybercriminal, who possesses intelligence, knowledge of information systems, and uses computerized means to harm the legal rights of others, taking advantage of a new universe of possibilities for criminal activity. Criminal law faces many difficulties adapting within this context.

Furthermore, the creation of specific criminal offenses aimed at data protection should to observe the principles of minimum intervention and proportionality. Criminal law should not to be used excessively, but only when civil and administrative sanctions apply. They prove insufficient to guarantee the protection of essential legal rights. In this sense, Costa Silva (2022) argues that the unlawful processing of personal data, when it causes harm Effective against the moral or economic integrity of the individual, it must be classified as a criminal offense. specific, with penalties gradations according to the degree of harm and the intent of the conduct.

RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

International experience reinforces this need, considering that several countries of the European Union, in accordance with the General Data Protection Regulation (GDPR), They foresee criminal penalties for serious cases of misuse of personal information, especially when there is intent or obtaining an illicit advantage. This trend demonstrates that criminal protection Data protection is a well-established reality in mature legal systems, where the protection of Privacy is understood as an extension of the dignity of the human person (Duarte, 2022).

In the Brazilian context, the proposal for new criminal offenses could include criminalization. specific to the illegal trade of personal data, the re-identification of information anonymized and the intentional leakage of sensitive data. Furthermore, it would be necessary to updating penalties for existing offenses to reflect their social impact and The economic impact of these behaviors. The creation of these criminal offenses would allow for greater consistency. systematic, ensuring more effective responses that are commensurate with the severity of the offenses. cybernetics.

The articulation between the LGPD (Brazilian General Data Protection Law) and criminal law should occur in a complementary manner and harmonious. In turn, the LGPD establishes a preventive and accountability system. administrative law, while criminal law acts as a last *resort,* ensuring the punishment of behaviors that are more socially reprehensible. This interaction should be guided by the principle of proportionality, in order to avoid the excessive use of criminal punishment and, at the same time, to ensure the effectiveness of the legal protection of personal data (Souza *et al.,* 2024).

Finally, the creation of new criminal offenses aimed at protecting personal data should not... It should not be seen as a mere punitive expansion, but as an instrument for updating policy. Criminal activity in the face of contemporary technological complexity. The advancement of illicit practices in The digital environment demands a penal system that is sensitive to new forms of harm to dignity and... Informational freedom, that is, more than punishing, the objective should be to promote a A culture of security, transparency, and responsibility in the use of data. With this, only through this legislative modernization, combined with institutional cooperation and digital education, It will be possible to consolidate a truly effective criminal protection system aligned with the values of Democratic Rule of Law.

4.1 Improving the tools for digital investigation and evidence gathering

Investigating cybercrimes requires technical and legal tools. specific measures that guarantee both the effectiveness of criminal prosecution and the observance of rights. fundamental. The digital environment introduces new evidentiary challenges, since the traces

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

Computer data can be easily tampered with, deleted, or transferred to servers in other countries. In this context, the improvement of investigative methods must occur in in accordance with the principles established by the General Data Protection Law (LGPD), especially those of purpose, necessity and proportionality (Silva; Novais, 2023).

The use of personal data in criminal investigations must observe limits. clear constitutional principles. The LGPD, by regulating the processing of information, provides parameters to avoid abuses in data collection and use. According to Souza et al. (2024, p. 18), "the protection of privacy does not preclude criminal investigation, but requires that it take place within objective criteria and under judicial control, ensuring a balance between security and "Freedom." Therefore, the use of data must always be linked to a legitimate purpose. and proportional to the seriousness of the crime being investigated.

Technological advancements also demand the adoption of more sophisticated digital forensic methodologies. sophisticated techniques such as IP traceability, metadata analysis, and the use of Artificial intelligence in forensics should be incorporated responsibly and supervised, avoiding the violation of individual rights. Damião and Novais (2024, p. 14) They emphasize that "the reliability of digital evidence depends on strict adherence to the chain of control." "custody, data integrity, and transparency of data acquisition methods." Therefore, This perspective reinforces the idea that the effectiveness of criminal prosecution is directly related to... legitimacy of the means used.

As pointed out by Lima (2024, pp. 34-35), see:

> Digital criminal investigation is a highly relevant topic in the current context. In view of the rise in cybercrime and the need to modernize
>
> Investigative practices for dealing with crimes involving technology. [...]
>
> However, digital criminal investigation faces several challenges, such as the volatility and manipulability of digital data, the need for rigorous protocols to ensure the integrity of evidence, and the difficulty of tracking changes in the data. [...]
>
> Therefore, protecting privacy and fundamental rights is a crucial aspect of the digital criminal process.

Therefore, another relevant aspect is the cooperation between national bodies and Internationally, cybercrimes largely transcend geographical borders. requiring integration between the Federal Police, the Public Prosecutor's Office, and the National Authority of Data Protection Authority (ANPD) and international organizations. On the other hand, with Brazil's accession... The Budapest Convention on Cybercrime, which is still under consideration, would represent progress. significant in this sense, by facilitating the exchange of information and the harmonization of procedures.

RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

Furthermore, investment in the technical training of experts and agents is essential. public. Interdisciplinary training in law, technology, and information security is fundamental for the authorities to understand the peculiarities of digital evidence and operate efficiently. The absence of this qualification compromises the validity of the processes and It fosters impunity.

Therefore, improving the tools for digital investigation and evidence gathering is crucial. It is not limited to technical improvement, but also involves the institutional and ethical strengthening of criminal prosecution. It is necessary to build an investigative model that combines efficiency. and respect for human rights, ensuring that the fight against cybercrime takes place under the pillars of legality, transparency and proportionality.

4.2 The importance of awareness and institutional dialogue for effective protection data penalty

The effectiveness of criminal protection of personal data does not depend exclusively on the creation of standards or the improvement of investigative tools, but also of social awareness and institutional dialogue among the various actors in the justice system. In this context, the consolidation of a data protection culture requires an understanding, by part of society and the State, that informational privacy constitutes a legal right. essential to human dignity and digital citizenship (Costa; Silva, 2022).

Indeed, digital education is a fundamental element in this process, since... Society needs to understand the risks associated with excessive sharing of information and the vulnerability of technological platforms.

According to Duarte (2022, p. 27), “the criminal protection of data will only be effective if accompanied by a collective awareness of responsibility for ethical and safe use. "Regarding personal information." This awareness should be promoted through policies. public, educational campaigns and institutional programs aimed at both citizens and to companies and public officials.

Dialogue between institutions within the justice system, such as the Public Prosecutor's Office and the Judiciary... The Judiciary, the Federal Police, and the National Data Protection Authority (ANPD) are another an essential pillar for the criminal protection of data, considering that integrated action allows the sharing of information, the standardization of procedures, and the construction of joint prevention and repression strategies

Damião and Novais (2024, p. 19) emphasize that “data protection is a challenge

RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

This is a cross-cutting issue that requires a coordinated response between state agencies and the private sector, otherwise...
to undermine the effectiveness of sanctions and compromise public trust in the digital environment.

In this scenario, the National Data Protection Authority (ANPD), in particular,
It plays a strategic role in mediating between the administrative and criminal spheres, since its function does not
It is not only supervisory, but also educational, and should promote good governance practices.
data and promote dialogue between the State and civil society. Therefore, closer ties between the
The ANPD (National Data Protection Authority) and the security forces can contribute to the early detection of illegal conduct and...
for the construction of a more integrated system of legal protection.

Furthermore, it is necessary to invest in the ethical and technical training of professionals working in this field.
In criminal prosecution, such as police officers, prosecutors, judges, and experts, need...
to understand the fundamentals of the LGPD (Brazilian General Data Protection Law) and its implications for criminal proceedings, avoiding
Misinterpretations and decisions that may violate constitutional guarantees. This
The integration of legal and technological knowledge is essential for strengthening
of an institutional culture committed to fundamental rights.

In addition to this, in the words of Lopes (2023, p. 167):

> The concrete execution of the search and seizure of digital evidence, in accordance with the constitutional model of due process, requires several reinterpretations of precautionary measures, their admissibility requirements, their procedure, and the illegality of evidence. Especially given the immense surveillance potential enabled by new technologies and the virtualization of current society, respect for the constitutional model of due process is indispensable for the rational control of the actions of those involved in criminal prosecution.

Finally, it is important to recognize that the criminal protection of personal data transcends the...
The legal field encompasses political and social dimensions. The challenge is not only to punish offenders,
but to consolidate a society that values privacy, digital security, and respect for
Human dignity. Ongoing dialogue between institutions, businesses, and citizens is the way forward.
to transform data protection into a collective commitment. In this way, Brazil
It will be able to advance in building a modern, balanced, and humane penal system, capable
to respond effectively and legitimately to the challenges of the digital age.

5. Final considerations

The analysis carried out throughout this article has made it possible to understand that the General Law of
The General Data Protection Law (LGPD) constitutes an essential milestone in consolidating data protection.
The legal framework for privacy in Brazil, especially in light of the increasing incidence of crimes.
Cybersecurity. Although the law is administrative in nature, its effects extend to the criminal field.
by establishing security, accountability, and prevention parameters. The LGPD contributes,

RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

Thus, in order to structure a normative system that seeks to balance development technological protection of fundamental rights, reinforcing the importance of informational self-determination and privacy as pillars of the Democratic State Right.

However, it was found that the Brazilian legal system still lacks integration. The regulatory relationship between the LGPD (Brazilian General Data Protection Law) and the Penal Code, especially in the classification of specific conducts, is significant. related to the illicit use of personal data. The currently existing criminal offenses, such as computer intrusion, online fraud, and violation of professional secrecy. They prove insufficient to encompass the new forms of digital crimes, which are evolving. in an accelerated and transnational manner. This legislative gap compromises the effectiveness of repression increases the feeling of impunity for offenses that affect millions. citizens.

In addition to typological deficiencies, technical and procedural challenges persist. significant in criminal investigations involving cyberspace. The difficulty of identifying the perpetrators, the volatility of digital evidence, and the need for cooperation. International obstacles require not only legislative reforms, but also Investments in training, infrastructure, and digital governance. Integrated action between the National Data Protection Authority (ANPD), the Public Prosecutor's Office and the police Specialized expertise is essential to making the fight against cybercrimes more effective.

The research also demonstrated that the effectiveness of the LGPD depends on a culture. Institutional compliance and accountability in data processing. The adoption of Compliance policies, the use of security technologies, and digital education are measures... indispensable for reducing vulnerabilities and preventing illegal activities. In this sense, the LGPD fulfills these requirements. not only a regulatory function, but also an educational one, promoting awareness. on the importance of information security for both the public and private sectors private.

It can therefore be concluded that the prevention and repression of cybercrimes require a Integrated legislative reform is needed, capable of aligning criminal law with the complexities of digital society. The creation of specific criminal offenses aimed at the improper handling of... personal data, with penalties proportionate to the seriousness of the conduct and effective mechanisms for International cooperation. Furthermore, strengthening the ANPD (National Data Protection Authority) and expanding its reach are recommended. of the partnerships between security agencies and the Judiciary, in order to guarantee greater Efficiency in the collection and preservation of digital evidence.

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

In summary, the LGPD represents a remarkable advance in the protection of rights.
fundamental in the virtual environment, but their full effectiveness depends on the articulation between
Prevention, education, and penal repression. The consolidation of a penal system compatible with...
In the information age, it is essential to ensure data privacy and security.
cease to be mere normative aspirations and become real and concrete guarantees, protected.
efficiently by the Brazilian State.

References

ALMEIDA, J. de J., MENDONÇA, AB, DO CARMO, GP, SANTOS, KS, SILVA, LM
M., & de AZEVEDO, RRD (2015). **Cybercrimes.** Caderno De Graduação - Ciências Humanas E
Sociais - UNIT - SERGIPE, 2(3), 215–236. Retrieved from https://periodicos.grupotiradentes.com/
cadernohumanas/article/view/2013

BRAZIL. Constitution (1988). **Constitution of the Federative Republic of Brazil.** Brasília, DF: Presidency of the
Republic. from the Available at in:
https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRAZIL. Decree-Law No. 2,848, of December 7, 1940. **Penal Code.** Official Gazette of the Union:
Section 1, Rio de Janeiro, DF, p. 23,911, Dec. 31, 1940. Available at: https://www.planalto.gov.br/
ccivil_03/decreto-lei/del2848compilado.htm.

BRAZIL. **Law No. 12,737, of November 30, 2012.** Provides for the criminalization of computer crimes;
amends Decree-Law No. 2,848, of December 7, 1940 – Penal Code; and provides other measures.
Official Gazette of the Union: Section 1, Brasília, DF, p. 1, Dec. 3, 2012.
Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.

BRAZIL. **Law No. 12,965, of April 23, 2014.** Establishes principles, guarantees, rights and duties for
the use of the Internet in Brazil. Official Gazette of the Union: Section 1, Brasília, DF, p. 1, April 24,
2014. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-
2014/2014/lei/l12965.htm.

BRAZIL. **Law No. 13,709, of August 14, 2018.** Provides for the protection of personal data and
amends Law No. 12,965, of April 23, 2014 (Marco Civil da Internet). Official Gazette of the Union:
Section 1, Brasília, DF, p. 59, August 15, 2018. Available at: https://www.planalto.gov.br/ccivil_03/
_ato2015-2018/2018/lei/l13709.htm.

COSTA, Emanuely Silva; SILVA, Raíla da Cunha. **Cybercrimes and police investigation. Teresina:
Public Prosecutor's Office of the State of Piauí, 2022.** Available at: https://www.mppi.mp.br/internet/
wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-
policial.pdf. Accessed on: October 3, 2025.

CUNHA, Vinícius Ferreira da, CORTIZO, Vitor Martins. **Cybercrimes: legal implications,
effectiveness of existing laws.** Revista Acadêmica Online, [S. l.], v. 9, n. 2, 2024.
Available at: https://revistaacademicaonline.com/index.php/rao/article/view/122. Accessed on: October 3, 2025.

Year V, v.2 2025 | Submission: October 23, 2025 | Accepted: November 25, 2025 | Publication: November 27, 2025

DAMIÃO, Alisson Santana; NOVAIS, Thyara Gonçalves. **Legal consequences of the LGPD for cybercrimes.** Ibero-American Journal of Humanities, Sciences and Education – REASE, São Paulo, v. 10, n. 11, Nov. 2024. Available at: https://periodicorease.pro.br/rease/article/download/17054/9549/41352. Accessed on: October 3, 2025.

DIAS, José Lucas da Costa. **The administrative sanctions of the LGPD, responsibility and compensation for damages: a perspective from the violation of personal data through irregular sharing and lack of information security.** 2021. [56] p. Undergraduate Thesis (Law) – Pontifical Catholic University of Goiás, Goiânia, Available at https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1648. Accessed on: November 7, 2025.

DUARTE, Karla Lorrany da Silva. **Cybercrimes and the impacts of the General Data Protection Law.** 2022. Monograph (Bachelor's Degree in Law) — Centro Universitário, Anápolis. Available at https://repositorio.aee.edu.br/bitstream/aee/20048/1/Karla%20Lorrany%20da%20Silva%20Duarte.pdf. Accessed on: October 3, 2025.

LIMA, Daniel Moura de. **Digital evidence in criminal investigation.** 2024. 77 p. Undergraduate Thesis (Bachelor of Laws) - National Faculty of Law, Federal University of Rio de Janeiro, Rio de Janeiro, 2024.

LOPES, Marcus Vinícius Pimenta. **The active participation of the accused in prosecution using the search and seizure of digital evidence.** 2023. 235 p. Thesis (Doctorate in Law) – Pontifical Catholic University of Minas Gerais, Belo Horizonte, 2023.

MACHADO, RLK. **Cybercrimes, invasion of privacy and the effectiveness of Brazilian legislation.** Projeção e Ciência, Brasília, v. 17, n. 2, p. 45-63, 2021. Available at: https://projecaociencia.com.br/index.php/Projecao2/article/view/1798. Accessed on: Oct. 3, 2025.

SILVA, Ronaldo Couto da; NOVAIS, Thyara Gonçalves. **The General Data Protection Law and its application in combating cybercrimes: challenges and perspectives.** Ibero-American Journal of Humanities, Sciences and Education – REASE, São Paulo, v. 9, n. 10, Nov. 2023. DOI: 10.51891/rease.v9i10.12254. Available at https://periodicorease.pro.br/rease/article/view/12254. Accessed on: October 3, 2025.

SOUZA, AP de; SIMAS, DC de S.; JUSTINIANO, J. dos S.; SOUZA JUNIOR, AM de; LIMA, JS de; NORTE, NNB de O.; NORTE FILHO, AF do; SALES, RAC de; SILVA, KAL da; BRITO, RM **Digital protection and consumer protection in the fight against cybercrimes.** Contribuciones a las Ciencias Sociales, [S. l.], v. 17, n. 10, p. e11454, Available 2024. https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/11454. Accessed on: Oct. 3, 2025. DOI: 10.55905/revconv.17n.10-134.

ZACARIAS, Fabiana; FREIRE, Lucas Zacharias. **Cybercrimes: an analysis of the difficulties and challenges.** JurES Journal, Vitória, v. 16, n. 29, p. 29-61, June 2023. Available at: https://estacio.periodicoscientificos.com.br/index.php/juresvitoria/article/download/1537/1628/2822. Accessed on: October 3, 2025.