RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/10/2026 | Accepted: 06/13/2026 | Publication: 06/16/2026

The Right to Privacy in the Digital Age: An Analysis of the Carolina Dieckmann Law

O Direito à Privacidade na Era Digital: Uma Análise da Lei Carolina Dieckmann

El Derecho a la Privacy en the Digital Era: An Analysis of it Carolina Dieckmann Law

Regina Barboza Lima – Catholic Faculty of Rondônia (FCR), Porto Velho-RO, Regina.lima@sou.fcr.edu.br
Ana Cláudia Miranda Lopes Assis – Catholic Faculty of Rondônia (FCR), ana.assis@fcr.edu.br

Abstract:
This article analyzes the right to privacy in the digital age based on Law No. 12.737/2012, known as the Carolina Dieckmann Law, examining its importance, its limits, and its articulation with the Brazilian system for the protection of intimacy, private life, and personal data. The research starts from the following problem: to what extent is the Carolina Dieckmann Law effective in protecting privacy in the digital environment in the face of technological evolution, new forms of cybercrime, and the constitutional expansion of the right to the protection of personal data? As a hypothesis, it is argued that the aforementioned law represented an indispensable milestone for the criminal protection of digital privacy, by criminalizing the invasion of computer devices, but its sufficiency is relative, since the protection of the person in cyberspace requires integrated interpretation with the Federal Constitution, the Civil Code, the Marco Civil da Internet (Brazilian Internet Bill of Rights), the General Law on the Protection of Personal Data, and subsequent legislation, such as Law No. 14.132/2021, which criminalized stalking. The overall objective is to evaluate the effectiveness of the Carolina Dieckmann Law in protecting digital privacy. Specific objectives include: understanding the evolution of the concept of privacy towards the notion of informational self-determination; analyzing the crime of unauthorized access to computer devices as defined in Article 154-A of the Penal Code; distinguishing the criminal protection of privacy from civil, constitutional, and administrative protections; and examining the challenges arising from practices such as phishing , data theft, improper disclosure of personal information, and cyberstalking . The methodology adopted is bibliographic and documentary, with a qualitative approach, based on the analysis of legislation, doctrine, and the normative context related to cybercrimes and the protection of personal data. It is concluded that the Carolina Dieckmann Law remains relevant as a starting point for the criminal protection of digital privacy, especially after the amendments introduced by Law No. 14.155/2021, which reinforced the criminal response to unauthorized access to computer devices. However, its effectiveness depends on a systemic and articulated understanding, capable of combining criminal repression, prevention, digital education, information security, civil liability, and personal data protection.

Keywords:
Cyberstalking . Cybercrimes. Right to privacy. Carolina Dieckmann Law. Personal Data Protection.

Resumo:
O presente artigo analisa o direito à privacidade na era digital a partir da Lei n.º 12.737/2012, conhecida como Lei Carolina Dieckmann, examinando sua importância, seus limites e sua articulação com o sistema brasileiro de proteção da intimidade, da vida privada e dos dados pessoais. A pesquisa parte do seguinte problema: em que medida a Lei Carolina Dieckmann é eficaz para proteger a privacidade no ambiente digital diante da evolução tecnológica, das novas formas de criminalidade cibernética e da ampliação constitucional do direito à proteção de

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/10/2026 | Accepted: 06/13/2026 | Publication: 06/16/2026

dados pessoais? Como hipótese, sustenta-se que a referida lei representou marco indispensável para a tutela penal da privacidade digital, ao tipificar a invasão de dispositivo informático, mas sua suficiência é relativa, pois a proteção da pessoa no ciberespaço exige interpretação integrada com a Constituição Federal, o Código Civil, o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais e legislações posteriores, como a Lei n.º 14.132/2021, que tipificou o crime de perseguição. O objetivo geral consiste em avaliar a eficácia da Lei Carolina Dieckmann na proteção da privacidade digital. Como objetivos específicos, busca-se: compreender a evolução do conceito de privacidade para a noção de autodeterminação informativa; analisar o crime de invasão de dispositivo informático previsto no art. 154-A do Código Penal; distinguir a proteção penal da privacidade das tutelas civil, constitucional e administrativa; e examinar os desafios decorrentes de práticas como phishing, roubo de dados, exposição indevida de informações pessoais e ciberstalking. A metodologia adotada é bibliográfica e documental, com abordagem qualitativa, fundada na análise da legislação, da doutrina e do contexto normativo relacionado aos crimes cibernéticos e à proteção de dados pessoais. Conclui-se que a Lei Carolina Dieckmann permanece relevante como ponto de partida da tutela penal da privacidade digital, especialmente após as alterações promovidas pela Lei n.º 14.155/2021, que reforçaram a resposta penal à invasão de dispositivo informático. Todavia, sua efetividade depende de uma compreensão sistêmica e articulada, capaz de combinar repressão penal, prevenção, educação digital, segurança da informação, responsabilização civil e proteção de dados pessoais.

Palavras-chave:
Ciberstalking. Crimes cibernéticos. Direito à privacidade. Lei Carolina Dieckmann. Proteção de Dados Pessoais.

Resumen:
El presente artículo analiza el derecho a la privacidad en la era digital a partir de la Ley n.º 12.737/2012, conocida como Ley Carolina Dieckmann, examinando su importancia, sus límites y su articulación con el sistema brasileño de protección de la intimidad, la vida privada y los datos personales. La investigación parte del siguiente problema: ¿en qué medida la Ley Carolina Dieckmann es eficaz para proteger la privacidad en el entorno digital frente a la evolución tecnológica, las nuevas formas de ciberdelincuencia y la ampliación constitucional del derecho a la protección de datos personales? Como hipótesis, se sostiene que dicha ley representó un hito indispensable para la tutela penal de la privacidad digital al tipificar la invasión de dispositivos informáticos; sin embargo, su suficiencia es relativa, ya que la protección de la persona en el ciberespacio exige una interpretación integrada con la Constitución Federal, el Código Civil, el Marco Civil de Internet, la Ley General de Protección de Datos Personales y legislaciones posteriores, como la Ley n.º 14.132/2021, que tipificó el delito de acoso. El objetivo general consiste en evaluar la eficacia de la Ley Carolina Dieckmann en la protección de la privacidad digital. Como objetivos específicos, se busca comprender la evolución del concepto de privacidad hacia la noción de autodeterminación informativa; analizar el delito de invasión de dispositivo informático previsto en el artículo 154-A del Código Penal; distinguir la protección penal de la privacidad de las tutelas civil, constitucional y administrativa; y examinar los desafíos derivados de prácticas como el phishing, el robo de datos, la divulgación indebida de información personal y el ciberacoso. La metodología adoptada es bibliográfica y documental, con enfoque cualitativo, fundamentada en el análisis de la legislación, la doctrina y el contexto normativo relacionado con los delitos cibernéticos y la protección de datos personales. Se concluye que la Ley Carolina Dieckmann sigue siendo relevante como punto de partida para la tutela penal de la privacidad digital, especialmente después de las modificaciones introducidas por la Ley n.º 14.155/2021, que reforzaron la respuesta penal frente a la invasión de dispositivos informáticos. No obstante, su efectividad depende de una comprensión

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/10/2026 | Accepted: 06/13/2026 | Publication: 06/16/2026

sistémica y articulada, capaz de combinar represión penal, prevención, educación digital, seguridad de la información, responsabilidad civil y protección de datos personales.

Palabras clave:
Ciberacoso. Delitos cibernéticos. Derecho a la privacidad. Ley Carolina Dieckmann. Protección de datos personales.

1. Introduction

Contemporary social relations have been profoundly transformed by advances in information and communication technologies. Activities previously restricted to physical space now take place in digital environments, such as social networks, messaging applications, storage platforms, banking systems, electronic public services, and computer devices connected to the internet. This new reality has expanded the possibilities for communication, access to information, and social participation, but has also intensified the risks of violations of privacy, private life, honor, image, and personal data [1].

In this scenario, the right to privacy, guaranteed by the 1988 Federal Constitution, has begun to face challenges specific to the digital society. Private life is no longer concentrated solely in physical spaces or material documents, but has become projected onto cell phones, computers, digital accounts, databases, online platforms, and networked communication systems. As a result, device intrusions, unauthorized access, exposure of images, unauthorized disclosure of personal information, phishing , credential theft, digital fraud, and cyberstalking have come to represent concrete threats to human dignity.

Historically, the Brazilian legal system has faced difficulties in criminally classifying certain behaviors committed in the computer environment. Before Law No. 12,737/2012, known as the Carolina Dieckmann Law, the invasion of devices and the improper obtaining of digital files were frequently analyzed based on traditional criminal offenses, which were not always adequate to the nature of the data and information stored electronically. This difficulty generated legal uncertainty, especially because digital data can be copied, reproduced, or shared without necessarily involving the physical removal of the asset.

Law No. 12,737/2012 therefore emerged as a relevant legislative response to a specific gap in Brazilian Criminal Law, by introducing the crime of unauthorized access to computer

[1]COPETTI, Rafael; MIRANDA, Marcel Andreata De. et al. **Informational Self-Determination and Data Protection: A Critical Analysis of Brazilian Jurisprudence. Law, governance and new technologies** . Florianópolis: CONPEDI, 2015. Available at: < http://www.egov.ufsc.br/portal/sites/default/files/j6023guzncw4in57.pdf > Accessed on: June 10, 2026.

devices into the Penal Code. Its enactment was prompted by a high-profile case involving the improper exposure of the privacy of a nationally known individual, highlighting the need for more adequate criminal protection against unauthorized access to personal devices and information.

Despite its historical importance, the Carolina Dieckmann Law cannot be analyzed in isolation. Technological evolution, the emergence of new forms of digital crime, and the expansion of the normative system for privacy protection demand an integrated interpretation. The Federal Constitution protects intimacy, private life, honor, and image; Constitutional Amendment No. 115/2022 included the protection of personal data as an autonomous fundamental right; the Marco Civil da Internet (Brazilian Internet Bill of Rights) establishes principles, guarantees, rights, and duties for internet use; the General Data Protection Law regulates the processing of personal data; and the Penal Code has undergone further updates, such as Law No. 14.155/2021, which amended Article 154-A, and Law No. 14.132/2021, which criminalized stalking.

Given this context, the central problem of this research is to investigate to what extent Law No. 12.737/2012 is effective in protecting privacy in the digital age, considering subsequent legislative changes, the constitutional autonomy of personal data protection, and the technical complexity of cybercrimes. The hypothesis adopted is that the Carolina Dieckmann Law represented an indispensable milestone for the criminal protection of digital privacy, but its sufficiency is relative, since the effective protection of the individual in the virtual environment depends on the articulation between criminal repression, civil protection, constitutional protection, information security, digital education, and the legal regime for the protection of personal data.

The overall objective of this study is to evaluate the effectiveness of the Carolina Dieckmann Law in protecting digital privacy. Specific objectives include: understanding the evolution of the concept of privacy towards the notion of informational self-determination; analyzing the crime of unauthorized access to a computer device as defined in Article 154-A of the Penal Code; examining the changes introduced by Law No. 14.155/2021; distinguishing between criminal protection of privacy and civil, constitutional, and administrative protections; and relating the Carolina Dieckmann Law to other relevant normative instruments, such as the Brazilian Internet Bill of Rights (Marco Civil da Internet), the Brazilian General Data Protection Law (LGPD), and the Stalking Law .

The methodology adopted is bibliographic and documentary in nature, with a qualitative approach. The research is based on the analysis of Brazilian legislation, specialized doctrine,

and norms related to the protection of privacy, personal data, and the fight against cybercrimes. The study starts from a legal-dogmatic perspective, seeking to understand the limits and possibilities of criminal protection of privacy in the digital environment, without disregarding the necessary articulation with other mechanisms for the protection of the individual.

The relevance of this research is justified by the increasing exposure of individuals to digital risks and the need to understand how the law can respond to new forms of violation of privacy and personal data. The analysis of the Carolina Dieckmann Law allows us to verify the advances made by the Brazilian legislature, but also highlights that the protection of privacy in the digital age does not depend solely on punishment after the invasion of devices. It also requires prevention, digital education, information security, civil and administrative liability, institutional cooperation, and strengthening the culture of personal data protection.

Beyond the invasion of computer devices, the research also addresses practices such as cyberstalking and the improper disclosure of personal information, as such conduct demonstrates that digital privacy can be violated both by unauthorized access to stored data and by repeated harassment, abusive surveillance, threats of information disclosure, and disruption of the victim's freedom in the virtual environment. This broadening of the debate is essential to understanding that contemporary legal protection should not be limited to the protection of electronic equipment, but must extend to the person, their privacy, their autonomy, their freedom, their psychological integrity, and their informational self-determination.

Therefore, this work seeks to demonstrate that the Carolina Dieckmann Law remains relevant for the criminal protection of digital privacy, but it must be understood as part of a broader normative ecosystem. The effectiveness of protecting individuals in the digital age depends on the interaction between the Federal Constitution, the Civil Code, the Marco Civil da Internet (Brazilian Internet Bill of Rights), the LGPD (Brazilian General Data Protection Law), the Penal Code, and specific legislation aimed at addressing new forms of violation of intimacy, private life, and personal data.

2. Theoretical Framework

2.1 Privacy, intimacy and protection of personal data in the digital society

The protection of privacy and intimacy is a fundamental right guaranteed by the 1988 Federal Constitution, especially in Article 5, item X, which recognizes the inviolability of intimacy, private life, honor, and image of individuals, ensuring compensation for material or

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/10/2026 | Accepted: 06/13/2026 | Publication: 06/16/2026

moral damages resulting from its violation. In the digital environment, this protection takes on special relevance, as private life has become projected onto computer devices, social networks, messaging applications, digital platforms, databases, and network communication systems.

Traditionally, the right to privacy has been understood from a negative perspective, associated with the "right to be left alone," that is, the protection of the individual against undue intrusions into their private sphere. However, this understanding has become insufficient in the face of the information society and the advancement of information and communication technologies.[2]

In the digital landscape, privacy has also come to involve an active dimension of control over personal information, encompassing the possibility for individuals to influence access, exposure, sharing, purpose, and use of data related to their personal lives.

This evolution leads to the notion of informational self-determination, understood as the right of a person to exercise control over their own data and personal information, monitoring and influencing how it is collected, used, stored, shared, and deleted. [3]Thus, the data subject ceases to be merely someone protected against undue intrusions and becomes recognized as an active subject in controlling the circulation of their information.

In this context, it is necessary to distinguish between privacy and personal data protection. Privacy protects the intimate sphere, private life, and personal privacy of an individual against undue exposure, interference, or intrusion. Personal data protection, in turn, encompasses any information related to an identified or identifiable natural person, even if that information is not, in itself, intimate or sensitive. Data such as name, CPF (Brazilian taxpayer ID), location, email address, access logs, browsing habits, and consumption profile may not directly reveal a person's intimacy, but their improper handling can affect their freedom, autonomy, dignity, and informational self-determination.

Constitutional Amendment No. 115/2022 consolidated this evolution by including in Article 5, item LXXIX, of the Federal Constitution, the fundamental right to the protection of

---

[2]DONEDA, Danilo Cesar Maganhoto . **From privacy to the protection of personal data: elements of the formation of the General Data Protection Law** . 2nd ed. São Paulo: Thomson Reuters Brasil, 2020. See also: COOLEY, Thomas McIntyre . **A treatise on the law of torts, or the wrongs which arise independent of contract** . Chicago: Callaghan and Company, 1879; WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy** . *Harvard Law Review* , v. 4, n. 5, p. 193-220, 1890.

[3]MENKE, Fabiano. **German origins and the meaning of informational self-determination** . *Migalhas* , October 30, 2020; DONEDA, Danilo Cesar Maganhoto . **From privacy to the protection of personal data** . 2nd ed. São Paulo: Thomson Reuters Brasil, 2020.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/10/2026 | Accepted: 06/13/2026 | Publication: 06/16/2026

personal data, including in digital media. [4]With this, data protection became expressly included in the catalog of fundamental rights, without being confused with privacy, although historically connected to it.

Thus, in the virtual environment, the protection of privacy, intimacy, and personal data is essential for preserving freedom and human dignity. The improper exposure of information, the hacking of devices, the misuse of data, and the lack of transparency in the handling of personal information can compromise not only an individual's private sphere, but also their autonomy, security, reputation, and capacity for free participation in social life.[5]

2.2 Civil-constitutional protection of digital privacy

In Brazil, the protection of privacy has a civil-constitutional foundation. This means that privacy should not be understood merely as an available individual interest or as a simple relationship between private individuals, but as a fundamental right linked to human dignity, freedom, intimacy, and the free development of personality.

At the constitutional level, Article 5, item X, of the Federal Constitution guarantees the inviolability of privacy, private life, honor, and image. Item XII of the same article also protects the secrecy of correspondence and telegraphic, data, and telephone communications, except in legal cases and by court order, when applicable. These provisions form the constitutional basis for the protection of private life, including in the digital environment.

In civil law, the Civil Code concretizes this protection through personality rights, establishing in Article 21 that the private life of a natural person is inviolable, authorizing the judge, at the request of the interested party, to adopt the necessary measures to prevent or stop any act contrary to this rule. Article 187 considers the abusive exercise of a right to be unlawful, especially when the holder exceeds the limits imposed by good faith, good morals, or the economic and social purpose of the right.

Thus, the invasion of computer devices, unauthorized access to personal accounts, unauthorized disclosure of images, abusive sharing of private information, and improper use of personal data can constitute not only criminal offenses but also civil offenses. In the criminal

---

[4]BRAZIL. **Constitutional Amendment No. 115, of February 10, 2022.** Amends the Federal Constitution to include the protection of personal data among fundamental rights and guarantees.

[5]RODOTÀ, Stefano. **Life in the Surveillance Society: Privacy Today** . Rio de Janeiro: Renovar, 2008; BIONI, Bruno Ricardo. **Regulation and Protection of Personal Data: The Principle of Accountability** . Rio de Janeiro: Forense, 2022.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/10/2026 | Accepted: 06/13/2026 | Publication: 06/16/2026

field, strict typification is required; in the civil field, protection is broader, as it seeks to prevent, cease, or remedy violations of personality rights.

This understanding is relevant to the present research because it demonstrates that the Carolina Dieckmann Law does not act in isolation. It is part of a broader system for the protection of individuals in the digital age, composed of the Federal Constitution, the Civil Code, the Marco Civil da Internet (Brazilian Internet Bill of Rights), the LGPD (Brazilian General Data Protection Law), and specific criminal laws aimed at addressing conduct in the virtual environment.

2.3 Regulatory framework for privacy protection in the digital environment

The Brazilian Internet Bill of Rights (Marco Civil da Internet), Law No. 12.965/2014, represents an important regulatory milestone for the discipline of internet use in Brazil. Its relevance stems from the fact that it establishes principles, guarantees, rights, and duties applicable to the digital environment, functioning as a normative framework aimed at the legal organization of relationships developed on the network.

This legislation is predominantly based on principles, aimed at establishing general parameters for internet use in the country. Article 3 of the Brazilian Internet Bill of Rights establishes, among its principles, the guarantee of freedom of expression, communication and manifestation of thought, the protection of privacy, the protection of personal data "as provided by law," the preservation and guarantee of net neutrality, the stability, security and functionality of the network, as well as the accountability of agents according to their activities.

For this reason, the Brazilian Internet Bill of Rights (Marco Civil da Internet) should not be treated as a general regime for the protection of personal data. It anticipates and structures essential principles for the protection of users' rights on the internet, creating a normative basis that was later expanded upon by the LGPD (Brazilian General Data Protection Law). In this sense, it can be understood as a kind of "Constitution of the Internet," establishing general foundations and guidelines for the digital environment, without replacing the specific technical discipline of personal data protection.[6]

---

[6]ASSIS, Ana Cláudia Miranda Lopes. **Digital compliance and data protection in elementary education: an analysis from the perspective of the LGPD regarding the challenges and perspectives for public education in the municipality of Porto Velho–RO** . 2024. Thesis (Doctorate in Law) – Pontifical Catholic University of Rio Grande do Sul, Porto Alegre, 2024. Available at: https://tede2.pucrs.br/tede2/handle/tede/12012 . Accessed on: May 14, 2026.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/10/2026 | Accepted: 06/13/2026 | Publication: 06/16/2026

The General Data Protection Law, Law No. 13.709/2018, in turn, represents the main Brazilian legal regime focused on regulating the processing of personal data. Its purpose is to protect the fundamental rights of freedom, privacy, and free development of the personality of the natural person, establishing rules applicable to processing operations carried out by natural or legal persons, of public or private law, in physical or digital media.11 [2]

The LGPD (Brazilian General Data Protection Law) is not criminal in nature and should not be understood as a generic privacy law. It is a technical, principled, and procedural norm aimed at regulating the activities of collection, storage, use, sharing, deletion, and other forms of processing of personal data. While the Carolina Dieckmann Law operates in the criminal field, by criminalizing the invasion of computer devices, the LGPD acts in a preventive, regulatory, administrative, and civil dimension, disciplining how personal data should be processed in a lawful, transparent, secure, and responsible manner.[7]

Among the principles of the LGPD (Brazilian General Data Protection Law), the following stand out: purpose, adequacy, necessity, free access, data quality, transparency, security, prevention, non-discrimination, and accountability. The law also guarantees the data subject rights such as confirmation of the existence of processing, access, correction, anonymization, blocking, deletion, portability, information about sharing, revocation of consent, and opposition to irregular processing.[1]

Therefore, the Brazilian Internet Bill of Rights (Marco Civil da Internet) and the General Data Protection Law (LGPD) perform distinct and complementary functions. The former establishes general principles for internet use; the latter technically regulates the processing of personal data. Both, however, are part of the same normative ecosystem for the protection of individuals in the digital environment.

2.4 Cybercrimes and criminal protection of privacy

Technological evolution has profoundly modified forms of social, economic, and communicational interaction, but it has also increased the risks of violating fundamental rights. The internet and computer devices have come to be used not only as instruments of

[7]BRAZIL. **Law No. 13.709, of August 14, 2018** , arts . 1, 5, 6, 7, 18, 42 and 46; PECK, Patrícia Pinheiro. **Personal Data Protection: comments on Law No. 13.709/2018 (LGPD)** . 4th ed. São Paulo: SaraivaJur , 2023.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/10/2026 | Accepted: 06/13/2026 | Publication: 06/16/2026

communication and access to information, but also as means for carrying out illicit conduct that affects the privacy, property, honor, freedom, and security of individuals.

Cybercrimes can be understood as criminally relevant conduct committed through the use of computers, computer networks, electronic devices, information systems, or digital environments. These means may function as instruments for committing the crime or constitute the very object of the criminal conduct.[8]

Legal doctrine typically distinguishes between proper and improper cybercrimes. Proper cybercrimes are those in which the digital environment , computer systems, or electronic data are integral to the crime itself, as in the case of hacking into a computer device. Improper cybercrimes, on the other hand, correspond to traditional crimes committed through the internet or digital technologies, such as fraud, threats, defamation, unauthorized disclosure of images, and other conduct that could occur outside the virtual environment but is amplified by technology.[9]

Digital crime presents specific challenges, such as the speed of execution of the acts, the rapid dissemination of information, the difficulty in identifying the perpetrators, the volatility of digital evidence, the transnational nature of certain practices, and the need for specialized expertise. These elements demonstrate that confronting cybercrimes requires not only criminal repression, but also prevention, digital education, information security, institutional cooperation, and constant legislative updates.[10]

2.5 The Carolina Dieckmann Law and the invasion of computer devices

Law No. 12,737/2012, known as the Carolina Dieckmann Law, represents a significant milestone in the evolution of criminal protection of digital privacy in Brazil. Its enactment occurred in a context of increasing exposure of individuals to risks arising from the use of computers, cell phones, social networks, applications, and other information devices, especially

---

[8]COLLI, Maciel. **Cybercrimes: limits and perspectives on police investigation of cybercrimes** . Curitiba: Juruá, 2010; ROSSINI, Augusto Eduardo de Souza. **Informatics, telematics and criminal law** . São Paulo: Memória Jurídica, 2004.

[9]WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Cybercrimes: threats and investigation procedures** . 2nd ed. Rio de Janeiro: Brasport , 2013; ROSA, Fabrizio Rosa. **Cybercrimes: penal and procedural aspects** . São Paulo: JH Mizuno, 2017.

[10]MARCELI, Vilma Maria; DAHER, Roberto José. **Evolutionary analysis of cybercrimes and Brazilian criminal law** . *FACP Electronic Journal* , year XV, no. 28, p. 100-116, Mar. 2026.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/10/2026 | Accepted: 06/13/2026 | Publication: 06/16/2026

given the absence, until then, of a specific criminal offense aimed at the invasion of devices and the improper obtaining of data or information stored digitally.[1]

The law introduced Article 154-A into the Penal Code, creating the criminal offense of unauthorized access to a computer device. The importance of this rule lies not only in protecting the electronic device itself, but also in safeguarding the data, information, images, communications, and personal records stored on it, which can reveal aspects of the user's privacy and private life.

Before Law No. 12.737/2012, actions such as computer hacking, unauthorized obtaining of digital files, or improper access to personal data were often analyzed based on traditional criminal offenses such as theft, violation of correspondence, damage, or interruption of service. However, this attempt at classification was not always adequate, as digital data has its own nature: it can be copied, reproduced, and shared without the victim necessarily losing physical possession of the file.[11]

The original wording of Article 154-A required that the intrusion occur "through the improper violation of a security mechanism." This requirement was criticized for restricting the application of the criminal offense to cases where the overcoming of a technical barrier was demonstrated. Subsequently, Law No. 14,155/2021 amended Article 154-A of the Penal Code, removing the express requirement of improper violation of a security mechanism from the main clause and shifting the focus of the analysis to the unauthorized intrusion into another person's computer device, with the specific purpose of obtaining, altering, or destroying data or information, or installing vulnerabilities to obtain an illicit advantage.[2] [1]

Law No. 14,155/2021 also increased the penalties applicable to the crime of unauthorized access to a computer system. This update demonstrates that the Carolina Dieckmann Law should be understood within a process of maturation of Digital Criminal Law, marked by the need to adapt to new forms of crime committed through technological means.[2] [2]

The sufficiency of the Carolina Dieckmann Law, therefore, must be interpreted relatively. The law was essential to fill a legislative gap and provide specific criminal treatment for the invasion of computer devices, but it is not sufficient, in isolation, to protect privacy in the digital age. Its effectiveness depends on its articulation with the Federal Constitution, the Civil Code, the Marco Civil da Internet (Brazilian Internet Bill of Rights), the LGPD (Brazilian General Data Protection Law), subsequent criminal laws, and digital security policies.

---

[11]PINHEIRO, Patrícia Peck. **Digital Law** . 7th ed. São Paulo: Saraiva, 2021.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/10/2026 | Accepted: 06/13/2026 | Publication: 06/16/2026

Thus, the Carolina Dieckmann Law proves to be adequate as a starting point for the criminal protection of digital privacy, but its normative force is revealed more consistently when understood as part of a legal ecosystem for the protection of the individual in the digital age.

2.6 Cyberstalking , improper disclosure of personal information and new violations of digital privacy.

cyberstalking and the improper disclosure of personal information stand out . These practices demonstrate that the violation of digital privacy occurs not only through the invasion of computer devices, but also through repeated harassment, abusive monitoring, and the unauthorized disclosure of data, images, conversations, or private information.

The Carolina Dieckmann Law, enacted at the end of 2012, represented the first significant response from the Brazilian Penal Code specifically addressing cybercrimes. It arose as a result of the impact of the case of the actress of the same name, whose computer was hacked, personal files were stolen, and intimate photos were released after extortion attempts. The main achievement of this law was the inclusion of Article 154-A in the Penal Code, which defined the crime of Computer Invasion, emphasizing that invading another person's computer device, whether or not connected to a computer network, through the undue violation of security mechanisms and with the purpose of obtaining, altering, or destroying data or information without the express or tacit authorization of the device's owner, constitutes a crime.

Before this law, accessing another person's cell phone or computer without permission to obtain personal data was not considered a crime. Victims had to resort to generic classifications or the civil sphere.

It is important to emphasize that the expression cyberstalking , also called cyber harassment , consists of repeated harassment carried out through digital means, such as social networks, messaging applications, emails, fake profiles, monitoring software, or other technological tools, with the aim of watching, harassing, threatening, intimidating, or disturbing the victim. The expression comes from the combination of *cyber* , relating to the digital environment, and *stalking* , a term of English origin used to designate persistent or obsessive harassment [12].

[12] MAIA, Daniel. **Criminalization of** stalking **in Brazil: analysis of article 147-** A **of the penal code in light of the right to privacy** . Available at: <https://repositorio.ufc.br/handle/riufc/73074 > Accessed on June 11, 2026.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/10/2026 | Accepted: 06/13/2026 | Publication: 06/16/2026

In the Brazilian legal system, stalking was criminalized by Law No. 14.132/2021, which added Article 147-A to the Penal Code [13]. This article punishes the act of repeatedly stalking someone by any means, threatening their physical or psychological integrity, restricting their freedom of movement, or otherwise invading or disturbing their sphere of freedom or privacy. By using the expression "by any means," the criminal offense also encompasses conduct carried out in the digital environment, such as persistent sending of messages, surveillance on social networks, creation of fake profiles, virtual threats, and undue monitoring.

The Carolina Dieckmann Law and the Stalking Law both protect aspects of digital privacy, but they address different types of conduct. The first focuses on suppressing the unauthorized invasion of another person's computer device, with the specific purpose of obtaining, altering, or destroying data or information, or installing vulnerabilities to obtain illicit advantage. The second focuses on repeated conduct that invades or disturbs the victim's freedom and privacy, even if there is no technical intrusion into the device.

In practice, these behaviors can coexist, such that the perpetrator can invade the victim's email, cell phone, or digital account to obtain photos, passwords, conversations, or personal data and subsequently use this information to repeatedly stalk, threaten, or harass them. In this scenario, the invasion of a computer device and digital stalking may constitute separate actions, depending on the specific case.

Also deserving of attention is the use of abusive monitoring software, known as *stalkerware* . This is spyware installed on a cell phone, computer, or other device to secretly monitor a person's activity without their consent. It can allow access to location, messages, calls, photos, emails, passwords, browsing history, and application usage. When used to access, monitor, or extract information from the victim's device, it may fall under Article 154-A of the Penal Code; if such information is used to stalk, threaten, or harass the victim, it may also fall under Article 147-A.

This relationship demonstrates that the protection of digital privacy cannot be reduced to the protection of the device, the system, or the password. The computer device is often merely the means by which profound aspects of a person's private life are accessed. Digital violation

[13]BRAZIL. Law No. 14,132, of March 31, 2021. **Adds article 147-A to Decree-Law No. 2,848, of December 7, 1940 (Penal Code), to provide for the crime of stalking; and repeals article 65 of Decree-Law No. 3,688, of October 3, 1941 (Law of Criminal Offenses)** . Available at: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm> Accessed on June 12, 2026.

can affect the intimacy, autonomy, freedom, reputation, tranquility, and psychological integrity of the victim.

The relationship between these two laws occurs in three main aspects: progression of conduct, means of execution, and the protected legal interest.

The means and the end: hacking as a tool of persecution. Device hacking, a conduct typified by the Carolina Dieckmann Law, is frequently used as a means of execution or escalation for the crime of cyberstalking .

Protection of privacy and intimacy. The protection of privacy, dignity, and individual freedom in the digital ecosystem is the common core of both laws. The Carolina Dieckmann Law guarantees the security of data present in the tools we use, while the Stalking Law safeguards the tranquility and self-determination of the individual against moral harassment and incessant virtual surveillance.

Historical and doctrinal evolution. Law 12.737/2012 allowed the Brazilian legislator to recognize that the virtual environment can increase psychological and moral harm. Cyberstalking is a direct consequence of this perception: it has been found that the virtual criminal does not limit himself to "invading the system" (as addressed by the Carolina Dieckmann Law), but frequently uses technology continuously to corner, monitor and harass the victim (as established by Law 14.132/2021).

The progress of Digital Law in Brazil is characterized by legislative responses to cases of violence and privacy violations that have moved to the virtual environment. The Carolina Dieckmann Law and the subsequent criminalization of cyberstalking are two important milestones in this trajectory. Although they address different behaviors, they share a significant historical, logical, and progressive connection [14].

Table 1 below shows a comparative summary of the two laws.

Table 1 – Comparative analysis of the Carolina Dieckmann Law vs. Law 14.132/2021

[14]FONTES, Jose Igor Alves. **Digital Personal Data and its Treatment in the Brazilian Legal System** . Undergraduate Thesis (Law) - UFRN. Natal/RN: CCS Sectoral Library, 2018. Available at: < https://monografias.ufrn.br/jspui/bitstream/123456789/7356/1/Dados%20Pessoais_Fontes_2018.pdf >. Accessed on: June 5, 2026.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/10/2026 | Accepted: 06/13/2026 | Publication: 06/16/2026

Criterion	Carolina Dieckmann Law (Art. 154-A)	Stalking / Cyberstalking Law (Art. 147-A)
Focus of Conduct	The act of hacking into a device by breaching its security to obtain/alter data.	The act of repeatedly stalking, generating fear or limiting the victim's freedom.
Temporality	It can be accomplished in a single act of invasion.	It requires regularity (repeated messages, monitoring, or attempts to contact).
Environment	Closely linked to computer devices.	It can occur in the physical environment, the digital (*cyber*) environment, or both cumulatively.

Source: The author, 2026

In summary, the Carolina Dieckmann Law ensured the legal protection of the "private digital space" (such as a cell phone or computer), while the criminalization of cyberstalking protects individuals against obsessive monitoring and harassment, both online and offline. The two work together to create a safer and less hostile digital environment for victims.

2.7 Current challenges for the protection of digital privacy

In the digital age, privacy challenges have become more complex due to the intense circulation of personal information on social networks, applications, digital platforms, databases, and automated systems. Massive data collection, lack of transparency regarding the

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/10/2026 | Accepted: 06/13/2026 | Publication: 06/16/2026

purposes of data processing, difficulty in obtaining truly informed consent, and the increase in data breaches are among the main problems faced by data subjects.[15]

The vulnerability of personal data does not only stem from sophisticated technical attacks, such as system intrusions or the installation of malicious programs. It also results from everyday practices, such as excessive sharing of information, use of weak passwords, automatic acceptance of terms of use, exposure of intimate or family images, filling out forms on insecure websites, and interaction with fraudulent links. Such situations create a favorable environment for phishing , identity theft, electronic fraud, computer device intrusion, improper exposure of images, and misuse of personal data.

Protecting privacy on social networks and digital platforms requires action on multiple fronts. It is the State's responsibility to enact appropriate regulations, oversee their application, and structure bodies capable of investigating and holding perpetrators of digital crimes accountable. At the same time, users, companies, and institutions must adopt preventive measures, information security strategies, and digital education programs, because protecting privacy is not achieved solely through punishment after the damage has occurred, but also through reducing the risks that facilitate the violation of personal data.

Beyond the preventive dimension, there are also significant legal challenges, since many digital crimes transcend national borders, making it difficult to define jurisdiction and hold perpetrators accountable. The collection of digital evidence also presents specific obstacles, as data can be deleted, altered, hidden, or stored on servers located in other countries. Added to this is the use of fake profiles, anonymization mechanisms, and other concealment technologies, which hinder the identification of those responsible.

Given this reality, combating cybercrime requires institutional and international cooperation. The Budapest Convention on Cybercrime, enacted in Brazil by Decree No. 11,491/2023, represents a relevant instrument for collaboration between States, especially considering the transnational nature of many crimes committed in the digital environment.[16]

Therefore, the protection of digital privacy cannot depend solely on criminal prosecution after the harm has occurred. It is necessary to combine prevention, digital education, information security, personal data protection, specialized investigation, institutional

---

[15]MEIRELES, Adriana Veloso. **Privacy in the 21st century: data protection, democracy and regulatory models** . *Brazilian Journal of Political Science* . Available at: https://www.scielo.br/j/rbcpol/a/my3M8sH3tfpm4WmXhrNcMjK/ . Accessed on: October 27, 2025.

[16]BRAZIL. **Decree No. 11,491, of April 12, 2023.** Promulgates the Convention on Cybercrime, signed in Budapest on November 23, 2001.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/10/2026 | Accepted: 06/13/2026 | Publication: 06/16/2026

cooperation, and civil, administrative, and regulatory mechanisms. Only an integrated response can provide greater effectiveness in protecting intimacy, private life, informational self-determination, and personal data in the digital society.

Speed is the main obstacle at the moment. Although the law requires a formal investigation procedure to prove authorship and the materiality of the crime, Artificial Intelligence makes it possible for the perpetrator to eliminate their traces, change their IP address, or create a new digital identity in a matter of seconds.

Thus, current protection focuses on proactive defense, rather than "reacting" (waiting for a crime to occur before prosecuting). This includes the use of multi-factor authentication (MFA), physical security keys, end-to-end encryption tools, and, most importantly, continuous digital education to recognize psychological fraud before a device is compromised.

3 final considerations

This study aimed to examine the right to privacy in the digital age through an analysis of Law No. 12.737/2012, known as the Carolina Dieckmann Law, evaluating its importance, its limits, and its place within the Brazilian legal framework for the protection of intimacy, private life, and personal data.

Throughout the research, it was found that privacy has undergone a significant conceptual transformation. Initially associated with the right to be left alone, in a more passive perspective of protection against undue intrusions, privacy has taken on a more active dimension in the digital society, related to control over the flow of personal information. In this context, the notion of informational self-determination gains relevance, whereby the individual must be able to understand and influence the collection, use, sharing, storage, and circulation of their data.

The Carolina Dieckmann Law represented a significant milestone for Brazilian Criminal Law, as it introduced the crime of unauthorized access to computer devices into the Penal Code, providing a specific normative response to a reality that had previously been insufficiently addressed by the legal system. Before its enactment, conduct involving unauthorized access to computers, cell phones, digital accounts, and personal files was frequently classified under traditional criminal offenses, which were not always adequate to the nature of the assets affected in the virtual environment.

However, the sufficiency of Law No. 12,737/2012 should be understood relatively. The law was essential as a starting point for the criminal protection of digital privacy, but it is not

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/10/2026 | Accepted: 06/13/2026 | Publication: 06/16/2026

capable, in isolation, of addressing all the risks inherent in the information society. The original wording of Article 154-A of the Penal Code required the undue violation of a security mechanism, which generated criticism regarding the limitation of its application. With the amendment introduced by Law No. 14,155/2021, this requirement ceased to be expressly stated in the main body of the provision, shifting the focus to the unauthorized invasion of another person's computer device, associated with the specific purpose of obtaining, altering, or destroying data or information, or installing vulnerabilities to obtain an illicit advantage.

This legislative change reinforced the criminal protection of digital privacy, including harsher applicable penalties. Even so, the protection of privacy in the virtual environment cannot depend exclusively on criminal prosecution after the harm has occurred. The speed of information dissemination, the difficulty in identifying perpetrators, the volatility of digital evidence, and the multiplicity of forms of violation demonstrate the need for a broader, more preventative, and integrated legal response.

In this context, the analysis of the Carolina Dieckmann Law must be articulated with other normative instruments. The Federal Constitution ensures the inviolability of intimacy, private life, honor, and image, and has also incorporated, through Constitutional Amendment No. 115/2022, the protection of personal data as an autonomous fundamental right. The Civil Code offers instruments for the prevention, cessation, and reparation of violations of personality rights. The Brazilian Internet Bill of Rights establishes principles, guarantees, rights, and duties for internet use in Brazil. The LGPD (Brazilian General Data Protection Law), in turn, technically regulates the processing of personal data, imposing duties of security, transparency, prevention, and accountability on data processing agents.

It has also been observed that new forms of privacy violation, such as cyberstalking and the improper disclosure of personal information, increase the complexity of the issue. Law No. 14.132/2021, by defining the crime of stalking, demonstrates that the protection of individuals in the digital environment is not limited to the defense of computer devices or stored data. Legal protection must also extend to the freedom, tranquility, psychological integrity, reputation, and security of the victim, especially in the face of repeated acts of surveillance, threats, coercion, or disturbance perpetrated through digital means.

It can be concluded, therefore, that the Carolina Dieckmann Law remains a relevant instrument for the criminal protection of digital privacy, but its effectiveness depends on updated interpretation and integration with the constitutional, civil, administrative, and regulatory system for the protection of the individual. Privacy in the digital age is not protected

by a single norm, but by a legal ecosystem composed of criminal, civil, constitutional, and personal data protection rules.

Therefore, protecting digital privacy requires not only punishing those responsible for hacking into computer devices, but also digital education, information security, risk prevention, proper preservation of evidence, civil and administrative liability, and strengthening the culture of personal data protection. The contemporary challenge lies in balancing technological innovation, freedom of internet use, and the protection of human dignity in cyberspace.

Finally, it is recommended that future studies delve deeper into the impacts of artificial intelligence, massive data collection, automated decisions, and new forms of digital surveillance on privacy and informational self-determination. Constant technological evolution imposes on the law the duty of permanent updating, so that the protection of intimacy, private life, and personal data remains effective in the face of new forms of violation in the digital environment.

References

ALMEIDA, Karen Rosa de. **Cyberstalking : from the current framework to the need for specific protection – an analysis in light of the Brazilian legal system and comparative law** . Available at: <https://periodicos.ufba.br/index.php/rppgd/article/download/36359/24988/175050> Accessed on October 25, 2025.

ASSUNÇÃO, Ana Paula Souza. **Cybercrimes** . Available at: <http://repositorio.aee.edu.br/bitstream/aee/538/1/Monografia%20-%20Ana%20Paula%20Souza.pdf> Accessed on October 22, 2025.

BARATTA, Alessandro. **Critical Criminology and Critique of Criminal Law: An Introduction to the Sociology of Criminal Law** . 3rd ed. Rio de Janeiro: Revan, 2002.

BIONI, Bruno. **Civil liability in the protection of personal data: building bridges between the General Law on the Protection of Personal Data and the Consumer Protection Code** . civilistica.com, v. 9, n. 3, p. 1-23, Dec. 22, 2020.

BISPO, Adrielle da Silva. **Cybercrimes: the ineffectiveness of the Carolina Dieckmann law in the practice of virtual crimes** . Available at: < https://periodicorease.pro.br/rease/article/download/12291/5727/23272> Accessed on October 28, 2025.

BRAZIL, 2018. **Law No. 13,709, of August 14, 2018.** Available at: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Accessed on October 2, 2025.

BRAZIL. **Law No. 8,078, of September 11, 1990.** Available at:

<http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm> Accessed on: October 20, 2025.

BRAZIL. **Decree-Law No. 3,914, of December 9, 1941.** Available at: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3914.htm> Accessed on October 17, 2025.

BRAZIL. Law No. 14,132, of March 31, 2021. **Adds article 147-A to Decree-Law No. 2,848, of December 7, 1940 (Penal Code), to provide for the crime of stalking; and repeals article 65 of Decree-Law No. 3,688, of October 3, 1941 (Law of Criminal Offenses)** . Available at: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm> Accessed on June 12, 2026.

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, Brasília, DF. December 3, 2012. Available at: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12737.htm > Accessed on: October 24, 2025.

COLHADO, Junyor Gomes. **Concept of crime in Brazilian Criminal Law** . Available at: <https://jus.com.br/artigos/47517/conceito-de-crime-no-direito-penalbrasileiro> Accessed on: March 7, 2025.

COPETTI, Rafael; MIRANDA, Marcel Andreata De. et al. **Informational Self-Determination and Data Protection: A Critical Analysis of Brazilian Jurisprudence. Law, governance and new technologies** . Florianópolis: CONPEDI, 2015. Available at: < http://www.egov.ufsc.br/portal/sites/default/files/j6023guzncw4in57.pdf > Accessed on: June 10, 2026.

DENNY, Danielle Mendes Thame et al., **International Law in the Age of Digital Populism** . Available at: <https://revista.internetlab.org.br/direito-internacional-na-erado-populismo-digital/> Accessed on October 29, 2025.

DONEDA, Danilo. **From privacy to the protection of personal data** . São Paulo: Thomson Reuters, 2019.

FERNANDES, Aloir de Araújo. **Crimes on the internet, the Carolina Dieckmann law and its flaws** . Available at: <https://ri.unipac.br/repositorio/wp-content/uploads/tainacanitems/282/137736/ALOIR-DE-ARAUJO-FERNANDES-CRIMES-NA-INTERNET-LEICAROLINA-DIECKMANN-DIREITO-2015.pdf> Accessed on October 30, 2025.

FONTES, Jose Igor Alves. **Digital Personal Data and its Treatment in the Brazilian Legal System** . Undergraduate Thesis (Law) - UFRN. Natal/RN: CCS Sectoral Library, 2018. Available at: < https://monografias.ufrn.br/jspui/bitstream/123456789/7356/1/Dados%20Pessoais_Fontes_2018.pdf >. Accessed on: June 5, 2026.

HINTZBERGEN, Jule. et al. **Fundamentals of Information Security: based on ISO 27001 and ISO 27002.** Translated by Alan de Sá. Rio de Janeiro: Brasport , 2018.

MACHADO, Rafael Lopes Kassem. CYBERCRIMES, INVASION OF PRIVACY AND THE EFFECTIVENESS OF THE STATE RESPONSE: the impacts of Law 12.737/2012 – Carolina Dieckmann Law and the General Data Protection Law in combating cybercrimes of invasion of privacy. Available at: <https://projecaociencia.com.br/index.php/Projecao2/article/download/1798/1444> Accessed October 20, 2025.

MAIA, Daniel. **Criminalization of** stalking **in Brazil: analysis of article 147-** A **of the penal code in light of the right to privacy** . Available at: <https://repositorio.ufc.br/handle/riufc/73074 > Accessed on June 11, 2026.

MASSON, Cleber. **Outlined Criminal Law** . Editora Método, São Paulo, 2009.

MEIRELES, Adriana **Veloso. Privacy in the 21st century: data protection, democracy and regulatory models** . Available at: <https://www.scielo.br/j/rbcpol/a/my3M8sH3tfpm4WmXhrNcMjK/ > Accessed on October 27, 2025.

MIRABETE, Julio Fabbrini; FABBRINI, Renato. **Manual of criminal law – general part** , v. I. 23rd ed. São Paulo: Atlas, 2006.

MUÉS, Gustavo Brandão Koury. **VIRTUAL CRIMES: An analysis of the adequacy of Brazilian criminal law** . Available at: <https://www.unirios.edu.br/revistarios/media/revistas/2018/18/crimes_virtuais.pdf> Accessed on: October 19, 2025.

NETTO, Thaís. **Information Security: Protection Mechanisms Within Organizations** . Available at: <https://direitoreal.com.br/artigos/seguranca-dainformacao-mecanismos-de-protecao-dentro-das-organizacoes> Accessed on: October 22, 2025.

OTOBONI, Gustavo Henrique dos Santos **. Cybercrimes: phishing . 2019.** Available at: <https://ambitojuridico.com.br/edicoes/revista191/crimesciberneticos-phishing/>. Accessed on October 26, 2025.

PEIXOTO, Andréa Stefani. **Data Protection Law: understand it in 13** points **!** Available at: <https://www.politize.com.br/lei-de-protecao-de-dados/ > 2020 , p. 43. Accessed on October 29, 2025.

PINHEIRO, Patrícia Peck. **Digital Law** . 7th ed. São Paulo: Saraiva, 2021.

ROSA, Fabrizio. **Computer Crimes** . Campinas: Bookseller , 2002.
SCHIMIDT, Guilherme. **Cybercrimes** . Available at: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Accessed on October 26, 2025.

SILVA, Márcio Ferreira da. **Effectiveness of the Carolina Dieckman Law** . Available at: <http://repositorio.aee.edu.br/bitstream/aee/17530/1/2017%20-

TCC%20-%20MARCIO%20FERREIRA%20DA%20SILVA.pdf> Accessed on October 30, 2025.

SILVA, Patrícia Santos da. **Cyber law and crime: an analysis of jurisdiction according to location in the trial of criminal cases** . Brasília: Vestnik , 2019.

SOUZA, Marcela Tavares et al. Integrative review: what it is and how to do it. **Revista Einstein** . v. 8, p.102-106, 2010. Available at: <http://www.scielo.br/pdf/eins/v8n1/pt_1679-4508-eins-8-1-0102.pdf.> Accessed on: October 20, 2025.

STEFAM, André. **Criminal Law: General Part** (Articles 1 to 120). São Paulo: Saraiva Educação, 2018.

TEIXEIRA, Tarcísio. **Digital Law and Electronic Process** . 5th ed. São Paulo: Saraiva, 2020.

VIEIRA, Waleska Duque Estrada. Privacy in the cyber environment: A fundamental right of the user. Revista **da ESMESC , v. 24, n. 30, p.** 197-217 , 2017. Available at: https://revista.esmesc.org.br/re/article/view/167 . Accessed on: May 10 , 2026. DOI : https://doi.org/10.14295/revistadaesmesc.v24i30.p197