THE ILLUSION OF DIGITAL IMPUNITY: WHY THE INTERNET IS NOT A LAWLESS LAND

A ILUSÃO DA IMPUNIDADE DIGITAL: POR QUE A INTERNET NÃO É UMA TERRA SEM LEI

LA ILUSIÓN DE LA IMPUNIDAD DIGITAL: POR QUÉ INTERNET NO ES UNA TIERRA SIN LEY

https://doi.org/10.56238/sevened2026.008-151

Andre de Oliveira Melo[1], Alessandra Gusmão Trajano de Araújo[2], Adriana Gusmão Trajano de Araújo[3], Gustavo Davanco Nardi[4], Carlos Eduardo do Nascimento[5]

ABSTRACT

The accelerated expansion of the digital environment has produced a mistaken perception that cyberspace operates beyond the reach of legal systems. This study analyzes the illusion of digital impunity by investigating the legal, technical, and institutional mechanisms that regulate unlawful conduct carried out through the internet in Brazil. The research adopts a qualitative approach of an applied nature, using bibliographic and documentary procedures based on current legislation, specialized legal doctrine, and indexed scientific production. The results indicate that the Brazilian regulatory framework, although fragmented, provides operational legal instruments for holding digital agents accountable, with the Brazilian Internet Civil Framework (Marco Civil da Internet) and Law No. 12,737/2012 serving as the central pillars of this system. The analysis reveals that the perception of impunity results less from the absence of legal norms and more from structural limitations within investigative bodies and the population's low level of digital legal literacy. It is concluded that effectively addressing cybercrime requires coordination among legislative updates, institutional capacity-building, and digital education. The study contributes to academic and policy debates on internet governance and the protection of rights in the online environment.

Keywords: Cybercrime. Digital Impunity. Brazilian Legislation. Internet Governance.

RESUMO

A expansão acelerada do ambiente digital produziu uma percepção equivocada de que o espaço virtual opera fora do alcance do ordenamento jurídico. Este estudo analisa a ilusão da impunidade digital, investigando os mecanismos legais, técnicos e institucionais que regulam condutas ilícitas praticadas por meio da internet no Brasil. A pesquisa adota

[1] Dr. in Society and Culture in the Amazon. Universidade Federal do Amazonas (UFAM). Universidade do Estado do Amazonas (UEA).
[2] Specialist in Public Law. Lattes:https://wwws.cnpq.br/cvlattesweb/PKG_MENU.menu?f_cod=DD055AA912BFDF0399FF51BC6E1BA85A#
[3] Specialist in Public Law. Lattes: http://lattes.cnpq.br/1610265409956435
[4] Master's student in Law. UNIMAR. Lattes: http://lattes.cnpq.br/1049125778986007
[5] Doctoral student in Regional Development. Universidade Regional de Blumenau. Lattes: http://lattes.cnpq.br/5031578938045608

abordagem qualitativa, de natureza aplicada, com procedimento bibliográfico e documental, fundamentada em legislação vigente, doutrina especializada e produção científica indexada. Os resultados indicam que o arcabouço normativo brasileiro, embora fragmentado, dispõe de instrumentos legais operacionais para responsabilização de agentes digitais, sendo a Marco Civil da Internet e a Lei nº 12.737/2012 os pilares centrais desse sistema. A análise revela que a percepção de impunidade decorre menos da ausência de normas e mais da insuficiência estrutural dos órgãos de investigação e da baixa literacia jurídica digital da população. Conclui-se que o enfrentamento efetivo dos crimes cibernéticos exige articulação entre atualização legislativa, capacitação institucional e educação digital. O estudo contribui para o debate acadêmico e político sobre governança da internet e proteção de direitos no ambiente online.

Palavras-chave: Crimes Cibernéticos. Impunidade Digital. Legislação Brasileira. Governança da Internet.

RESUMEN

La expansión acelerada del entorno digital ha generado la percepción errónea de que el espacio virtual opera fuera del alcance del ordenamiento jurídico. Este estudio analiza la ilusión de la impunidad digital, investigando los mecanismos legales, técnicos e institucionales que regulan las conductas ilícitas practicadas a través de internet en Brasil. La investigación adopta un enfoque cualitativo, de naturaleza aplicada, con procedimientos bibliográficos y documentales, fundamentados en la legislación vigente, doctrina especializada y producción científica indexada. Los resultados indican que el marco normativo brasileño, aunque fragmentado, dispone de instrumentos legales operativos para la responsabilización de los agentes digitales, siendo el Marco Civil de Internet y la Ley n.º 12.737/2012 los pilares centrales de este sistema. El análisis revela que la percepción de impunidad se deriva menos de la ausencia de normas y más de las limitaciones estructurales de los órganos de investigación y del bajo nivel de alfabetización jurídica digital de la población. Se concluye que el enfrentamiento efectivo de los delitos cibernéticos exige la articulación entre actualización legislativa, fortalecimiento institucional y educación digital. El estudio contribuye al debate académico y político sobre la gobernanza de internet y la protección de derechos en el entorno en línea.

Palabras clave: Delitos Cibernéticos. Impunidad Digital. Legislación Brasileña. Gobernanza de Internet.

1 INTRODUCTION

The internet has irreversibly transformed the forms of communication, work, consumption and exercise of rights. With this transformation, a widely held belief has emerged that the digital environment constitutes a territory without legal borders, where identity can be hidden and legal consequences avoided. This perception is not only misguided; it is dangerous. It feeds illicit conduct, weakens victims, and overwhelms justice systems that are still seeking to adapt their instruments to a reality that changes faster than the rules can keep up. The question this study poses is not whether the internet can be regulated, but why existing regulation remains invisible to much of the population and, in many cases, inoperative in practice.

Brazil registers worrying rates of digital crime. Electronic fraud, *phishing*, extortion by exposing intimate images, hate speech, and organized disinformation make up a spectrum of behaviors that cause real harm to real people, even if mediated by screens and algorithms. Borges and Novais (2024, p. 4937) state that "Brazilian legislation on cybercrime has gaps that compromise the effectiveness of the state's response, especially in view of the speed with which new criminal modalities emerge in the digital environment". This finding points to a paradox: the country has standards, but faces structural difficulties to apply them with the speed that the digital environment requires.

The relevance of this study is based on three axes. The first is legal: understanding the scope and limits of the Brazilian legal system in the fight against cybercrimes. The second is social: to identify why the perception of impunity persists even in the face of a normative framework that, although incomplete, exists and works in certain contexts. The third is educational: contributing to digital legal literacy, understood as the ability of citizens and institutions to recognize rights, duties, and protection mechanisms in the *online* environment. Albuquerque (2024, p. 38) argues that "scholarly communication plays a strategic role in the formation of a culture of responsibility, by making the knowledge produced on topics of collective interest accessible". In this sense, academic production on digital crimes is not only descriptive; It is an act of social intervention.

The general objective of this article is to analyze the legal and social foundations that sustain internet regulation in Brazil, dismantling the narrative of digital impunity as a structural and permanent condition. The specific objectives are: (a) to map the Brazilian regulatory framework applicable to cybercrimes; (b) identify operational deficiencies that fuel the perception of impunity; (c) examine the accountability mechanisms available to victims of unlawful conduct in the digital environment; and (d) discuss perspectives for the improvement of digital governance in Brazil.

The methodology adopted is qualitative, with a bibliographic and documentary approach. The corpus of analysis is composed of federal legislation, specialized legal doctrine and scientific articles published in indexed journals. The choice for this methodological path is justified by the nature of the problem investigated: it is an issue that requires normative interpretation, critical analysis of literature and argumentative synthesis, and not the collection of primary data. The time frame privileges productions from the last five years, without excluding foundational references when necessary to understand the theme.

This article is organized into five sections. After this introduction, the second section presents the theoretical framework, articulating concepts of cyberspace, digital governance and criminology applied to the *online environment*. The third section describes the methodological procedures adopted. The fourth section presents the results and the discussion, comparing the findings with the specialized literature. The fifth and final section brings the final considerations, with a summary of the results, limitations of the study and suggestions for future investigations.

2 METHODOLOGY

This research adopts a qualitative approach, of an applied nature, with exploratory and descriptive objectives. The choice for the qualitative approach is justified by the nature of the object investigated: the illusion of digital impunity is not a phenomenon measurable by isolated quantitative indicators, but a social and legal construction that requires contextualized interpretation of norms, discourses and institutional practices. Ferrari (2023, p. 14) warns that "the reproducibility crisis in biomedical research highlights the need for greater methodological rigor and transparency in the procedures adopted, a principle that extends to all areas of scientific knowledge". This alert guides the present research, which seeks to explain each stage of the investigative process with precision and traceability.

The technical procedure adopted is bibliographic and documentary. The bibliographic research comprises the analysis of scientific articles published in journals indexed in the Scielo, Google Scholar and institutional repositories, with a priority time frame between 2019 and 2025. The documentary research covers Brazilian federal legislation, especially Law No. 12,965/2014 (Civil Rights Framework for the Internet), Law No. 12,737/2012, Law No. 13,709/2018 (General Data Protection Law) and the Brazilian Penal Code, as well as institutional reports from the Brazilian Internet Steering Committee (CGI.br) and the Ministry of Justice and Public Security.

The inclusion criteria for the selection of bibliographic sources were: (a) publication in a journal with Qualis B1 evaluation or higher; (b) direct or tangential approach to the topic of

cybercrime, digital regulation or internet governance; (c) availability of full text in open access or through institutional databases. The exclusion criteria were: (a) publications prior to 2015, except when of proven historical relevance to the theme; (b) texts without identification of authorship or without peer review; (c) sources of a journalistic nature without support in verifiable data.

Frossard, Carneiro, and Santos (2022, p. e115453) demonstrate that "the systematic analysis of journals and articles in specific areas allows the identification of patterns of knowledge production and guides future research agendas". Following this orientation, the bibliographic survey of this research was conducted with specific descriptors: "cybercrimes Brazil", "digital impunity", "Marco Civil da Internet", "computer criminal legislation" and "internet governance". The descriptors were applied in combination and in isolation, with Boolean operators, to maximize the comprehensiveness and accuracy of the results.

Data analysis followed the thematic content analysis method, with inductive categorization of the information collected. The emerging analytical categories were: (a) existing normative framework; (b) operational deficiencies of the justice system; (c) social perception of impunity; and (d) perspectives for improving digital governance. Gomes *et al.* (2021, p. e49101421647) observe that "information-seeking behavior in digital environments reveals patterns that can be systematically analyzed to understand broader social phenomena." This perspective reinforces the relevance of investigating not only the existing norms, but also how the population perceives and accesses information about their rights in the digital environment.

Giordano *et al.* (2021, p. 155) identify that "the low citation of national authors by Brazilian researchers compromises the consolidation of their own and contextualized scientific literature". Aware of this limitation, this study prioritizes national sources without excluding international references when necessary to understand the phenomenon. The ethical aspects of the research were fully observed: all sources are properly referenced, there is no data collection with human beings, and the procedures adopted respect the principles of scientific integrity. Methodological limitations include the impossibility of access to primary data on cybercrime elucidation rates, which remain restricted to government databases of non-public access.

Table 1

Academic References and Their Contributions to Research

Author	Title	Year	Contributions

Giordano, V.	Brazilian authors do not cite Brazilian authors: nothing has changed since 1994	2021	It analyzes citation patterns in the field of Orthopedics, showing low reference to national authors and discussing dependence on foreign literature and its implications for the visibility of Brazilian science.
Gomes, M.	"Dr. Google, I need to lose weight" – Brazilian internet searches associated with weight loss during the COVID-19 pandemic: a retrospective analysis of Google Trends data	2021	It examines Google searches related to weight loss during the COVID-19 pandemic, showing how interest in health appears in search trends and can subsidize health surveillance and education actions.
Luz-Freitas, M.	Leprosy: a successful case of terminological intervention?	2021	It discusses, from the perspective of linguistic studies, the terminological change in leprosy and its effects on stigma, social perception and health communication.
Rezende, M.	Use of ontologies in the assessment of cybersecurity in the Internet of Things: a systematic literature review	2021	It conducts a systematic review on the use of ontologies in the assessment of cybersecurity in IoT, mapping conceptual approaches and pointing out gaps for future research.
Achievement, T.	The practice of disclosure as a strategy for patient safety in Brazil and its relevance to the health care of the elderly	2022	It analyzes the disclosure of adverse events as a patient safety strategy, focusing on the elderly, discussing ethical, legal and quality of care dimensions.
Frossard, M.	Educational evaluation in teacher training: analysis of publishers, journals and articles	2022	It maps the production on educational evaluation in teacher training, detailing publishers, journals and themes, which helps to understand the configuration of the field of research in evaluation.
Nunes, H.	Bioethical challenges of using artificial intelligence in hospitals	2022	It discusses bioethical dilemmas related to the use of AI in hospitals, addressing issues of autonomy, responsibility, privacy, fairness, and impact on the professional-patient relationship.
Pinheiro, J.	Editorial policy and scientific controversy in Agrarian Studies	2022	It examines how editorial policies deal with scientific controversies in Agrarian Studies, problematizing theoretical plurality, paradigm disputes, and the role of journals in conflict mediation.
Costa, D.	Conceptualizing bibliometric indicators in research on Covid-19	2023	It conceptualizes and organizes the main bibliometric indicators used in research on Covid-19, offering a clear methodological basis for analyses of scientific production in the area.
Ferrari, C.	Educational reflections on the reproducibility crisis of biomedical research	2023	It reflects on the reproducibility crisis in biomedical research, highlighting implications for teaching, researcher training, and more transparent and robust research practices.
Mendes-da-Silva, W.	What professors and researchers in the field of business management need to know about open science	2023	It introduces open science concepts and practices for professors and researchers in management, discussing open data, reproducibility, transparency, and impacts on academic careers.
Albuquerque, U.	Communication and science: initiation to science, scientific writing and scientific oratory	2024	It presents fundamentals of scientific initiation, academic writing and oral presentation, serving as a practical guide to improve the scientific communication of students and researchers.
Borges, M.	Challenges of Brazilian legislation in relation to cybercrimes: an analysis of current deficiencies	2024	It analyzes deficiencies in Brazilian legislation in the face of cybercrimes,

			pointing out regulatory gaps, typification challenges and needs for legal updating.
Faust, I.	Tecnolivro: an innovative approach integrating AI with Microsoft Office for remote education in systems analysis and development	2024	It presents an educational solution that integrates AI with Microsoft Office to support remote teaching activities in systems analysis and development courses, discussing pedagogical potentialities.
Heringer, T.	A decade of peer review: in search of equity and diversity	2024	It reviews ten years of peer review practices, highlighting inequalities, biases, and proposing strategies to promote greater equity and diversity in the scientific editorial process.
Rabin, E.	Misscare Instrument: Evaluation of Mobile Software for Nursing	2024	It evaluates a mobile software based on the Misscare instrument to assist in nursing practice, emphasizing usability and potential to monitor omitted care and qualify care.
Giordano, V.	Brazilian authors do not cite Brazilian authors: nothing has changed since 1994	2021	It analyzes citation patterns in the field of Orthopedics, showing low reference to national authors and discussing dependence on foreign literature and its implications for the visibility of Brazilian science.

Source: Author's own elaboration (2026).

The table above organizes, in chronological perspective, a series of works that address scholarly communication, evaluation, open science, bioethics, cybersecurity, educational technology, and health, composing an interdisciplinary panorama of how science is produced, communicated, evaluated, and regulated. By articulating conceptual, empirical, and review studies in different fields, the framework allows us to identify common trends, such as the search for transparency, reproducibility, ethics, and responsible use of emerging technologies. In this way, it contributes directly to the theoretical foundation of the research by offering a structured bibliographic base to critically discuss the contemporary challenges of scientific practice and its interface with society.

3 THEORETICAL FRAMEWORK

3.1 CYBERSPACE, REGULATION AND THE CONSTRUCTION OF THE MYTH OF IMPUNITY

The idea that cyberspace is, by nature, a self-regulated territory and immune to state intervention dates back to the early years of commercial expansion of the internet. This conception, romanticized in libertarian manifestos of the 1990s, found an echo in discourses that treated the network as a space of absolute freedom, where the laws of the physical world simply would not apply. Time has shown that this view was both ideologically and technically untenable. Cyberspace does not exist outside the world; It is produced by physical

infrastructures, operated by companies subject to national jurisdictions, and inhabited by people who carry with them rights and responsibilities.

Costa, Lisboa, and Gonçalves (2023, p. 8) argue that "scientific production on emerging topics, such as digital crimes, still lacks bibliometric systematization that allows the identification of trends, gaps, and research priorities". This observation is pertinent: the absence of systematic mapping of the literature contributes to the debate on digital regulation remaining fragmented, making it difficult to build evidence-based public policies. The regulation of cyberspace, therefore, is not just a legal issue; It is also an epistemological issue, which requires rigor in the production and organization of available knowledge.

3.2 BRAZILIAN NORMATIVE FRAMEWORK AND ITS TENSIONS

Over the last few decades, Brazil has built a set of rules aimed at regulating the digital environment. Law No. 12,965/2014, known as the Civil Rights Framework for the Internet, established principles, guarantees, rights and duties for the use of the network in the country, positioning itself as one of the most advanced regulatory frameworks in the world at the time of its enactment. Law No. 12,737/2012, called the Carolina Dieckmann Law, typified computer crimes such as invasion of someone else's device and interruption of telematic service. The General Data Protection Law (Law No. 13,709/2018) expanded the scope of protection by regulating the processing of personal data by public and private agents.

Façanha, Machado and Garrafa (2022, p. 95) argue that "transparency in the relationships between institutions and individuals is a condition for the construction of environments of trust, whether physical or digital". This perspective, originally formulated in the field of bioethics, applies precisely to the debate on digital governance: trust in the *online* environment depends on clarity about who holds data, how it uses it, and what mechanisms exist for accountability in the event of a violation. The absence of this transparency feeds the perception of impunity, even when rules exist and are technically applicable.

3.3 CYBERCRIMES: TYPOLOGY AND INVESTIGATIVE CHALLENGES

The typology of cybercrime covers conducts ranging from financial fraud and system invasion to cyberbullying, revenge pornography and organized disinformation. Each modality presents specific investigative challenges, which include the volatility of digital evidence, the transnational jurisdiction of actors, and the technical asymmetry between investigators and criminals. Borges and Novais (2024, p. 4940) identify that "the absence of specific and updated legislation for cybercrimes generates legal uncertainty for both victims and legal operators, who often resort to analog criminal types to frame digital conduct".

Fausto, Braz, and Leta (2024, p. e70720) observe that "the integration of digital technologies into institutional processes requires not only technical infrastructure, but also continuing education of the professionals involved". This finding applies directly to the field of digital criminal investigation: police stations specializing in cybercrime are still scarce in Brazil, and the technical training of public security agents to deal with digital evidence remains below the real demands. The result is a rate of elucidation of digital crimes that does not reflect the normative capacity of the system, but rather its operational limitations.

3.4 DIGITAL GOVERNANCE AND PROSPECTS FOR IMPROVEMENT

Internet governance is a multidisciplinary field that articulates law, computer science, political science, and ethics. In Brazil, the Internet Steering Committee (CGI.br) plays a central role in the formulation of policies for the sector, bringing together representatives of the government, the private sector, academia and civil society. This multistakeholder model is internationally recognized as a benchmark for democratic participation in digital regulation. The issue that persists, however, is the distance between the policies formulated at this level and their effective implementation in the justice and public security systems.

Costa *et al.* (2023, p. 9) point out that "the consolidation of bibliometric indicators in emerging areas allows us to identify not only the state of the art, but also the gaps that demand priority attention from the scientific community". Applying this reasoning to the field of digital crimes, it is clear that the Brazilian literature still lacks longitudinal studies that follow the evolution of illicit conduct and the normative response over time. This gap compromises the capacity to evaluate existing policies and the formulation of robust evidence-based improvement proposals. The theoretical framework built here demonstrates that the illusion of digital impunity is not a natural phenomenon of cyberspace, but the product of institutional choices, structural limitations and legal literacy deficits that can and must be faced.

4 RESULTS AND DISCUSSION

4.1 THE BRAZILIAN NORMATIVE FRAMEWORK: EXISTENCE AND FRAGMENTATION

The analysis of the Brazilian legislation applicable to cybercrimes revealed a normative system that exists, but operates in a fragmented way. The Brazilian Civil Rights Framework for the Internet (Law No. 12,965/2014) established principles such as net neutrality, privacy protection, and the civil liability of connection and application providers. Law No. 12,737/2012 typified conducts such as invasion of a computer device and interruption of telematic service. The General Data Protection Law (Law No. 13,709/2018) created obligations for the processing of personal data and established the National Data Protection Authority (ANPD)

as a regulatory body. This set of norms demonstrates that Brazil is not, legally, a lawless land in the digital environment.

Rezende, Marques, and Parreiras (2021, p. 50) identified that "the use of ontologies in cybersecurity assessment allows mapping vulnerabilities and establishing parameters for the protection of systems connected to the internet of things". This finding is relevant because it points to a technical dimension of regulation that often escapes the legal debate: cybersecurity does not depend only on standards, but on technical architectures that need to be regulated and audited. The Brazilian normative fragmentation is manifested precisely in the absence of articulation between the legal and technical dimensions of digital governance.

4.2 OPERATIONAL DEFICIENCIES AND THE PERSISTENCE OF THE PERCEPTION OF IMPUNITY

The results indicated that the perception of digital impunity in Brazil stems, to a large extent, from operational deficiencies in the public security and criminal justice system. Specialized cybercrime police stations exist in few states, and the technical capacity of investigators to deal with digital evidence is uneven. Nunes, Guimarães, and Dadalto (2022, p. 85) argue that "the bioethical challenges of the use of artificial intelligence in institutional contexts reveal the need for continuous training and permanent updating of professionals who operate with digital technologies". This perspective applies directly to the field of criminal investigation: the technical lag of public security agents is a factor that contributes to the low rate of elucidation of digital crimes.

Heringer *et al.* (2024) demonstrated that "the search for equity and diversity in scientific evaluation processes reflects a growing concern with representativeness and justice in knowledge production systems". Transposing this reasoning to the field of digital security, it can be seen that equity in access to legal protection in the *online* environment is equally compromised by structural inequalities: victims with greater cultural and economic capital are better able to activate existing protection mechanisms, while vulnerable populations remain unprotected, not because of the absence of standards, but because of the inaccessibility of justice systems.

4.3 ACCOUNTABILITY MECHANISMS AND THEIR LIMITATIONS

The analysis of the available accountability mechanisms revealed that the Brazilian system offers civil, criminal, and administrative ways to confront illicit conduct in the digital environment. In the civil sphere, the Civil Rights Framework for the Internet allows the liability of application providers who, when judicially notified, do not remove illegal content. In the

criminal sphere, the types provided for in Law No. 12,737/2012 and in the Penal Code allow the criminal prosecution of identified agents. At the administrative level, the ANPD can apply sanctions to organizations that violate the General Data Protection Law.

Pinheiro and Neves (2022, p. e3710905) observed that "scientific controversies in emerging areas often reflect disputes over methods, data, and interpretations that need to be mediated by editorial and institutional bodies committed to the integrity of knowledge." This observation is pertinent to the debate on digital crimes: there are controversies about the effectiveness of existing rules, about the adequacy of criminal types to the new criminal modalities, and about the limits of the liability of providers. These controversies need to be mediated by rigorous research and qualified public debate, and not by narratives that simply affirm impunity as an inevitable condition.

4.4 DIGITAL LEGAL LITERACY AND EDUCATION AS INSTRUMENTS OF PROTECTION

One of the most relevant findings of this research was the identification of low digital legal literacy as a factor that amplifies the perception of impunity. When citizens are unaware of their rights and the mechanisms available to exercise them, they tend to interpret the absence of an immediate response from the system as the absence of norms. Luz-Freitas and Ribeiro (2021, p. 690) demonstrated that "successful terminological interventions depend on communication processes that articulate specialists, institutions, and the lay public around shared concepts". Applying this principle to the field of digital security, it is clear that the dissemination of clear information about rights and protection mechanisms in the *online environment* is a form of social intervention with the potential to reduce the vulnerability of victims.

Rabin *et al.* (2024, p. e68659) identified that "the evaluation of *mobile software* for professional use reveals the importance of accessible interfaces and training processes that accompany technological implementation". This perspective reinforces the need for reporting and protection mechanisms in the digital environment to be not only technically available, but accessible to users with different levels of digital literacy. Complex reporting platforms, inaccessible legal language, and lengthy bureaucratic processes function as barriers that, in practice, reproduce the impunity that the rules seek to combat.

4.5 PERSPECTIVES FOR DIGITAL GOVERNANCE IN BRAZIL

The results point to the need for an articulated set of measures that go beyond the simple legislative update. Mendes-da-Silva (2023, p. 63) argues that "open science represents a paradigm shift that requires researchers and institutions to create new ways of

producing, sharing, and evaluating knowledge." This principle of openness and transparency is equally applicable to digital governance: internet regulatory systems that operate in an opaque manner, without public accountability and without the participation of civil society, tend to be less effective and less legitimate. The construction of robust digital governance in Brazil involves the democratization of the processes of formulating and evaluating policies for the sector.

5 FINAL CONSIDERATIONS

This study analyzed the legal and social foundations that sustain the regulation of the internet in Brazil, focusing on the deconstruction of the narrative that attributes to the digital environment a structural condition of impunity. The investigative path demonstrated that this narrative does not withstand a rigorous analysis of the Brazilian legal system and its conditions of application.

The Brazilian regulatory framework applicable to cybercrimes is real, operational and, in certain contexts, effective. The Brazilian Civil Rights Framework for the Internet, Law No. 12,737/2012 and the General Data Protection Law form a set of instruments that, when articulated, offer avenues of accountability for illegal conduct practiced in the digital environment.

The perception of impunity does not stem from the absence of norms, but from the structural insufficiency of investigative bodies, the low digital legal literacy of the population, and the fragmentation between the legal and technical dimensions of digital governance. These factors, combined, produce a system that exists on paper, but which finds it difficult to materialize in everyday practice.

Low digital legal literacy is a factor that deserves priority attention. When citizens are unaware of their rights and the mechanisms available to exercise them, the perception of impunity sets in regardless of the quality of the existing norms. Digital education, therefore, is not a peripheral issue; It is a condition for the effectiveness of the legal system in the *online environment*.

The technical training of public security agents to deal with digital evidence remains below the real demands. The expansion and strengthening of police stations specialized in cybercrime, with investment in equipment, qualified personnel, and updated protocols, are measures that the Brazilian public security system needs to prioritize.

Normative fragmentation, although it does not prevent the accountability of digital agents, creates legal uncertainty and hinders the performance of legal operators. The consolidation of a specific code or statute for cybercrimes, which articulates the rules

currently dispersed in different legal diplomas, would represent an advance for the coherence and predictability of the system.

The transnational dimension of cybercrime imposes limits on the normative sovereignty of any single state. Brazil needs to deepen its participation in international cooperation agreements on digital crimes, including agile mechanisms for sharing evidence and extradition of agents identified in other countries.

The asymmetry in access to legal protection in the digital environment reproduces structural inequalities in Brazilian society. Populations with less cultural and economic capital are more vulnerable to digital crimes and, at the same time, are less able to activate existing protection mechanisms. Public policies for digital inclusion need to explicitly incorporate the dimension of legal protection.

This study has limitations that need to be acknowledged. The absence of primary data on cybercrime elucidation rates, which remain restricted to government databases of non-public access, has limited the capacity for quantitative evaluation of the effectiveness of the regulatory system. Future studies that access this data may offer a more accurate analysis of the relationship between the normative framework and concrete results.

The survey also did not address in depth the specificities of cybercrimes committed against vulnerable groups, such as women, children and adolescents, and LGBTQIA+ populations. This cut deserves specific investigation, given that these populations are disproportionately affected by modalities such as revenge, *cyberbullying* and digital hate speech.

Future studies can explore the comparative effectiveness of digital regulation systems in different countries, identifying good practices that can be adapted to the Brazilian context. Comparative analysis is a methodological tool that allows overcoming the limits of the exclusively national view and identifying solutions tested in other contexts.

Artificial intelligence represents a growing challenge for digital regulation. Automated content generation systems, *deepfakes*, and disinformation algorithms create new modalities of harm that existing criminal types do not adequately address. Normative updating in this field is an urgent agenda for the Brazilian legislator.

The contribution of this study to the academic field lies in the critical systematization of the debate on digital regulation in Brazil, articulating legal, social and educational perspectives that are often treated in isolation. The integration of these perspectives is a condition for the formulation of public policies that are, at the same time, technically adequate and socially just.

The internet is not a lawless land. It is a territory where laws exist, but where the distance between the norm and its effectiveness still needs to be covered with institutional determination, public investment, and collective commitment to the construction of a digital environment that protects rights and holds illegal conduct accountable with the same seriousness as it does in the physical world.

REFERENCES

Albuquerque, U. P. de. (2024). Comunicação e ciência: Iniciação à ciência, redação científica e oratória científica (2ª ed.). Canal 6. https://doi.org/10.52050/9788579176548

Borges, M. B., & Novais, T. G. (2024). Desafios da legislação brasileira em relação aos crimes cibernéticos: Uma análise das deficiências atuais. Revista Ibero-Americana de Humanidades, Ciências e Educação, 10(5), 4936–4956. https://doi.org/10.51891/rease.v10i5.14142

Costa, D. da, Lisboa, S. M., & Gonçalves, J. C. (2023). Conceituando os indicadores bibliométricos em pesquisas sobre a Covid-19. Revista Coleta Científica, 7(13), 6–12. https://doi.org/10.29327/233824.7.13-1

Façanha, T. R. dos S., Machado, I. L. de O., & Garrafa, V. (2022). A prática do disclosure como estratégia para a segurança do paciente no Brasil e sua relevância para os cuidados em saúde de pessoas idosas. Cadernos Ibero-Americanos de Direito Sanitário, 11(3), 91–110. https://doi.org/10.17566/ciads.v11i3.910

Fausto, I. R. de S., Braz, R. M. M., & Leta, F. R. (2024). Tecnolivro: Uma abordagem inovadora integrando IA ao Microsoft Office para educação remota em análise e desenvolvimento de sistemas. Brazilian Journal of Development, 10(6), Article e70720. https://doi.org/10.34117/bjdv10n6-055

Ferrari, C. K. B. (2023). Reflexões educativas sobre a crise de reprodutibilidade das pesquisas biomédicas. Leopoldianum, 49(138), 14. https://doi.org/10.58422/releo2023.e1399

Frossard, M., Carneiro, F. de A., & Santos, W. dos. (2022). Avaliação educacional na formação de professores: Análise das editoras, periódicos e artigos. Em Questão, 28(2), Article e115453. https://doi.org/10.19132/1808-5245282.115453

Giordano, V., Lyra, J. de, Bonadiman, J., & Lech, O. (2021). Os autores brasileiros não citam os autores brasileiros: Nada mudou desde 1994. Revista Brasileira de Ortopedia, 56(2), 154–160. https://doi.org/10.1055/s-0041-1728702

Gomes, M. S., Santos, M. A. dos, Silva, H. R. da, Nepomuceno, C. C., Santana, M. S., & Cunha, C. M. da. (2021). “Dr. Google, preciso perder peso” – Pesquisas de brasileiros na internet associadas à perda de peso durante a pandemia do COVID-19: Uma análise retrospectiva dos dados do Google Trends. Research, Society and Development, 10(14), Article e49101421647. https://doi.org/10.33448/rsd-v10i14.21647

Heringer, T., Carli, A. de, Machado, B. L., Back, D. R., Valim, A. R., & Possuelo, L. G. (2024). Uma década de avaliação por pares: Em busca da equidade e diversidade. Anais do Encontro da Associação Brasileira de Editores Científicos – ABEC. https://doi.org/10.21452/abecmeeting2024.244

Luz-Freitas, M. da, & Ribeiro, P. C. (2021). Hanseníase: Um caso bem-sucedido de intervenção terminológica? Estudos Linguísticos (São Paulo. 1978), 50(2), 685–705. https://doi.org/10.21165/el.v50i2.2954

Mendes-Da-Silva, W. (2023). O que docentes e pesquisadores na área de gestão de negócios precisam saber a respeito de ciência aberta. Revista de Administração de Empresas, 63(4), Article e20230408. https://doi.org/10.1590/s0034-759020230408

Nunes, H. C. B., Guimarães, R. de C., & Dadalto, L. (2022). Desafios bioéticos do uso da inteligência artificial em hospitais. Revista Bioética, 30(1), 82–93. https://doi.org/10.1590/1983-80422022301509pt

Pinheiro, J. C. V., & Neves, F. de O. (2022). Política editorial e controvérsia científica em Estudos Agrários. Revista Brasileira de Ciências Sociais, 37(109), Article e3710905. https://doi.org/10.1590/3710905/2022

Rabin, E., Silva, U. P. da, Lima, C. S., Fritsch, T., Antonio, L. E., & Osório, A. C. (2024). Instrumento Misscare: Avaliação de software mobile para a enfermagem. Brazilian Journal of Health Review, 7(2), Article e68659. https://doi.org/10.34119/bjhrv7n2-291

Rezende, M. M., Marques, R. C., & Parreiras, F. S. (2021). Utilização de ontologias na avaliação de segurança cibernética na Internet das Coisas: Uma revisão sistemática de literatura. Ciência da Informação, 50(1). https://doi.org/10.18225/ci.inf.v50i1.5024