SEVEN
publicações acadêmicas

CYBERCRIMES FROM A SCIENTIFIC PERSPECTIVE: AN INTEGRATIVE REVIEW OF NATIONAL AND INTERNATIONAL PRODUCTION

CIBERCRIMES SOB A PERSPECTIVA CIENTÍFICA: REVISÃO INTEGRATIVA DA PRODUÇÃO NACIONAL E INTERNACIONAL

LOS CIBERDELICIOS DESDE UNA PERSPECTIVA CIENTÍFICA: UNA REVISIÓN INTEGRADORA DE LA PRODUCCIÓN NACIONAL E INTERNACIONAL

https://doi.org/10.56238/sevened2025.029-067

Daniel Braga da Silva[1], Adriana Conrado de Almeida[2], Carmen Silvia Arraes de Alencar Valença[3], Clarissa Alencar de Macau Furtado[4], Histephane Maria Bezerra de Vasconcelos[5], Luina Alencar Trajano[6], Marta Victor de Araujo[7], Betise Mery Alencar Sousa Macau Furtado[8]

ABSTRACT

Objective: To conduct an integrative review of the scientific literature published between 2019 and 2025 on cybercrimes, with an emphasis on the sociodemographic profile of victims and the characteristics of the offenses. Methodology: An integrative literature review was conducted according to the Prisma flowchart. The topic was initially defined, followed by searches in the Scopus, PubMed, Medline, Lilacs, SciELO, SciELO Brasil, Latindex, and PlumX Metrics databases. The Boolean operator "AND" and the keywords "cybercrimes," "cybercrime," "cybercrimes," and "internet crimes" were used, with no language restrictions. Inclusion criteria were articles published between 2019 and 2025, with free access, and that presented victims' sociodemographic data. Duplicate articles, literature reviews, dissertations, theses, books, documents, and studies without abstracts were excluded. Results: Of the 2,207 papers initially identified, 20 met the eligibility criteria and were read in full. Of these, six scientific articles comprised the final sample for analysis and discussion. The findings highlighted the growth and diversification of cybercrimes, with particular emphasis on electronic fraud through phishing, digital theft, and social media password theft.

[1] Master in Forensic Expertise. Universidade de Pernambuco (UPE). E-mail: danielbraga.silva@upe.br
Orcid: https://orcid.org/0009-0009-4844-3138 Lattes: http://lattes.cnpq.br/2495010715300669
[2] Dr. in Maternal and Child Health. Instituto de Medicina Integral Professor Fernando Figueira (IMIP).
E-mail: adriana.almeida@upe.br Orcid: https://orcid.org/0000-0001-6141-0458
Lattes: http://lattes.cnpq.br/3892527052352252
[3] Doctorate student in Forensic Expertise. Universidade de Pernambuco (UPE).
E-mail: carmen.valença@upe.br Orcid: https://orcid.org/0000-0002-6430-9707
Lattes: http://lattes.cnpq.br/8764643264668578
[4] Medical Student. Faculdade de Ciências Médicas Afya. E-mail: clarissamacau@gmail.com
Orcid: ORCID: https://orcid.org/0009-0004-3070-767X Lattes: http://lattes.cnpq.br/0589563486101637
[5] Master's student in Forensic Expertise. Universidade de Pernambuco (UPE). E-mail: hmbvlife@hotmail.com
Orcid: https://orcid.org/0009-0007-3081-6691 Lattes: http://lattes.cnpq.br/468803671225616
[6] Master's student in Forensic Expertise. Universidade de Pernambuco (UPE). E-mail: luinalencar@gmail.com
Orcid: https://orcid.org/0009-0005-6244-8163 Lattes: http://lattes.cnpq.br/0463740047240711
[7] Master's student in Forensic Expertise. Universidade de Pernambuco (UPE). E-mail:
marta.victoraraujo@upe.br
Orcid: https://orcid.org/0009-0003-2484-892X Lattes: http://lattes.cnpq.br/2929512073508593
[8] Dr. in Sciences. Fundação Oswaldo Cruz. E-mail: betisemery@gmail.com
Orcid: https://orcid.org/0000-0001-6344-8257 Lattes: http://lattes.cnpq.br/4682659587643054

Cybercrimes affected different countries and victim profiles, such as women and the elderly. Conclusion: The integrative review proved effective in achieving the proposed objectives, allowing for a more in-depth discussion on cybercrimes in national and international contexts, enabling us to identify the most frequent digital crimes and the profiles of their victims. Furthermore, the results highlight the need for constant adaptation of the digital society to new types of crimes, enhanced by technology, which can affect individuals and organizations at any time.

Keywords: Cybercrimes. Cyberspace. Cybersecurity. Interdisciplinarity.

RESUMO

Objetivo: Realizar uma revisão integrativa da literatura científica publicada entre 2019 e 2025 sobre cibercrimes, com ênfase no perfil sociodemográfico das vítimas e nas características das infrações. Metodologia: Revisão integrativa da literatura, conduzida de acordo com o fluxograma Prisma. Inicialmente, definiu-se o tema e, em seguida, realizaram-se buscas nas bases de dados Scopus, PubMed, Medline, Lilacs, SciELO, SciELO Brasil, Latindex e PlumX Metrics. Utilizou-se o operador booleano “AND” e as palavras-chave cibercrimes, cybercrime, crimes cibernéticos e crimes na internet, sem restrição de idioma. Como critérios de inclusão, artigos publicados entre 2019 e 2025, de acesso gratuito, que apresentassem dados sociodemográficos das vítimas. Foram excluídos artigos duplicados, revisões de literatura, dissertações, teses, livros, documentos, estudos sem resumo. Resultados: Dos 2.207 trabalhos inicialmente identificados, 20 atenderam aos critérios de elegibilidade e foram lidos integralmente. Desses, 6 artigos científicos compuseram a amostra final para análise e discussão. Os achados evidenciaram o crescimento e a diversificação dos cibercrimes, com destaque para o estelionato fraude eletrônica por meio da técnica phishing, furto digital e roubo de senhas de redes sociais, além de afetaram diferentes países e perfis de vítimas, por exemplo, as mulheres e pessoas idosas. Conclusão: A revisão integrativa mostrou-se eficaz para atingir os objetivos propostos, permitindo aprofundar o debate sobre cibercrimes em contextos nacionais e internacionais, no qual foi possível verificar os delitos digitais mais frequentes, bem como o perfil das vítimas. Além disso, os resultados ressaltam a necessidade de constante adaptação da sociedade digital frente a novas modalidades de delitos, potencializadas pelas tecnologias, que podem atingir indivíduos e organizações a qualquer momento.

Palavras-chave: Cibercrimes. Ciberespaço. Cibersegurança. Interdisciplinaridade.

RESUMEN

Objetivo: Realizar una revisión integrativa de la literatura científica publicada entre 2019 y 2025 sobre ciberdelitos, con énfasis en el perfil sociodemográfico de las víctimas y las características de los delitos. Metodología: Se realizó una revisión integrativa de la literatura según el diagrama de flujo Prisma. Inicialmente se definió el tema, seguido de búsquedas en las bases de datos Scopus, PubMed, Medline, Lilacs, SciELO, SciELO Brasil, Latindex y PlumX Metrics. Se utilizó el operador booleano "AND" y las palabras clave "ciberdelitos", "ciberdelito", "ciberdelitos" y "delitos en internet", sin restricciones de idioma. Los criterios de inclusión fueron artículos publicados entre 2019 y 2025, de libre acceso, que presentaran datos sociodemográficos de las víctimas. Se excluyeron artículos duplicados, revisiones bibliográficas, disertaciones, tesis, libros, documentos y estudios sin resúmenes. Resultados: De los 2207 artículos identificados inicialmente, 20 cumplieron con los criterios de elegibilidad y fueron leídos en su totalidad. De estos, seis artículos científicos constituyeron

la muestra final para su análisis y discusión. Los hallazgos destacaron el crecimiento y la diversificación de los delitos cibernéticos, con especial énfasis en el fraude electrónico mediante phishing, el robo digital y el robo de contraseñas en redes sociales. Los delitos cibernéticos afectaron a diferentes países y perfiles de víctimas, como mujeres y personas mayores. Conclusión: La revisión integradora resultó eficaz para lograr los objetivos propuestos, permitiendo una discusión más profunda sobre los delitos cibernéticos en los contextos nacional e internacional, lo que nos permitió identificar los delitos digitales más frecuentes y los perfiles de sus víctimas. Además, los resultados resaltan la necesidad de una adaptación constante de la sociedad digital a los nuevos tipos de delitos, potenciados por la tecnología, que pueden afectar a personas y organizaciones en cualquier momento.

Palabras clave: Delitos Cibernéticos. Ciberespacio. Ciberseguridad. Interdisciplinariedad.

1 INTRODUCTION

The internet was created in the mid-1960s as a military resource during the context of the Cold War. In Brazil, its arrival took place at the end of the 1980s. It became public and marketed between 1994 and 1995. According to the National Household Sample Survey, in 2021, approximately 90% of Brazilian households had access to the internet and pointed out by the Brazilian Institute of Geography and Statistics (IBGE, 2021).

The importance of the internet in the lives of people around the world is notorious, since it is a facilitating tool in everyday life, in addition to allowing the dissemination of news freely through the world wide web (WEB). Similar to the real world, illicit practices emerge in this environment, similar to those capitulated in the Penal Code, such as crimes against honor, the dignity of the human and sexual person, racial prejudice, supremacist ideas, electronic fraud, among others (PINHEIRO, 2021). These crimes are now called cybercrimes, understood as infractions committed in the virtual world, thus showing the transformation from the traditional to the digital form of crime (ARSAWATI ET AL., 2021). Historically, the first computer-aided offense was in 1958, in the United States of America, in which a Minneapolis bank employee altered a bank's programs to deposit small amounts of cents resulting from millions of financial transactions and, in 1966, the first conviction by an American federal court for the manipulation of bank data was recorded (MCQUADE, 2006).

The positive aspects of electronic media and virtual communication are widely recognized, as they facilitate the approximation between people through digital connection, in addition to favoring professional performance, especially with the popularization of remote work (home office). Therefore, many cyber criminals or cybercriminals act under the false premise that the virtual environment or cyberspace is exempt from laws or rules, believing that they can commit crimes without facing legal consequences. This environment is understood as an environment in constant transformation, marked by multiple forms of social and technological interaction (SOUZA, 2021).

In cyberspace, there is a democratization regarding the recognition of the criminological profile called haters, hackers and cybercriminals who commonly operate cyberattacks, when these attacks are related to information systems, or when computers or the internet are used as a means for criminal action or cybercrime (LORENZO; SCARAVELLI, 2021). Cybercriminals are following the advance of the hyper-connected digital society on the network, with strategic impacts through the manipulation of programs, using the failures of virtual protection means for illicit practices (TURGAL, 2023).

It is estimated that Brazil suffered 328,326 cyberattacks in the first half of 2023 and, in the second half of the same year, about 357,422 attacks, with emphasis on wireless telecommunications (MAIA, 2024). From the perspective of the world panorama, Brazil ranked fifth from April 2024 among the countries that suffered cyberattacks through ransomware, a way of hijacking victims' digital information. Thailand appears in first place (44.1%), followed by the United States (24.3%), Turkey (8.8%), Germany (2.7%) and Brazil with (1.8%) (TREND MICRO, 2024).

In view of the above and in order to contribute to the academic literature, the present study aimed to carry out an integrative review of the scientific literature published between 2019 and 2025 on cybercrimes, with an emphasis on the sociodemographic profile of the victims and the characteristics of the infractions, in order to understand and deepen knowledge, in addition to offering empirical subsidies for the formulation of public policies aimed at the prevention and repression of cybercrimes.

2 METHODOLOGY

An integrative literature review was used in this study in order to analyze and systematize the existing academic production on the subject, considering that this type of study ensures methodological rigor and a consistent critical analysis of the selected publications (SOUZA; SILVA; CARVALHO, 2020). The literature search ran from November 2024 to June 30, 2025. For the selection of publications in the databases, the following keywords were used: cybercrimes, cybercrimes, cybercrimes, and internet crimes, in the Scopus, PubMed, Medline, Lilacs, Scielo, Scielo Brazil, Latindex, and PlumX Metrics databases for the period from 2019 to 2025.

There is a duality regarding the use of the word cybercrime with i and y. The nomenclature with y for cybercrime was a priori defended by Susman and Heuston (1995), but effectively used in 1997 when it dealt with the report of the presidential commission, in which it was gathered for studies related to the protection of critical infrastructure (MCQUADE, 2006). In this research, the terminology cybercrime with i, defended by Jonathan Clough and ordered in the Budapest Convention (CLOUGH, 2010), will be used.

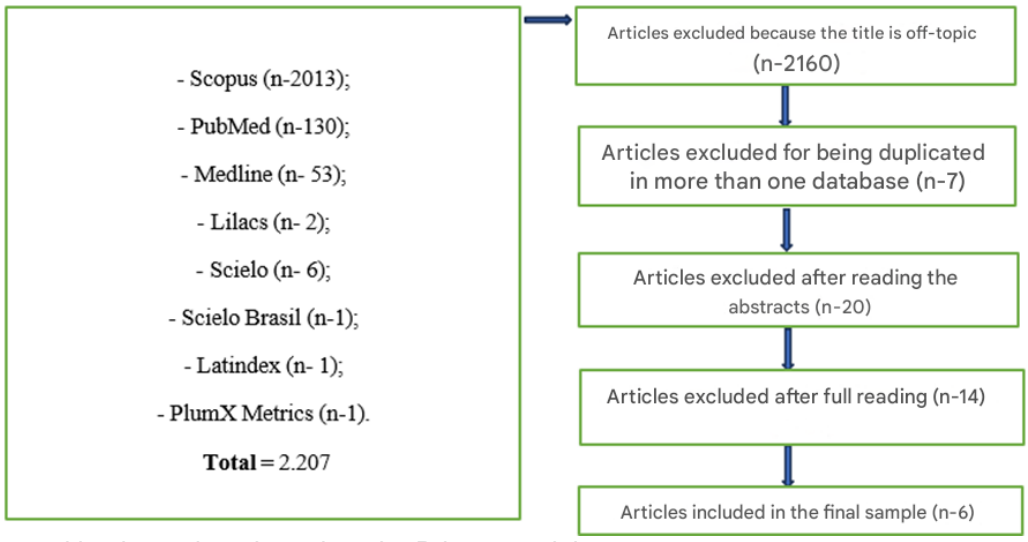
Articles published in the study period were considered as inclusion criteria; with free access; in any language. Duplicate articles in more than one database were excluded; literature reviews, letters to the editor, theses, dissertations, book chapters and official

documents on the subject. For a greater breadth of the search, the Boolean operator AND was used.

Of the total of 2,207 (two thousand two hundred and seven) studies initially identified, 2,160 were excluded because they were not within the theme after reading the titles. 47 remained, of which 7 were excluded because they were duplicates, in more than one database, leaving 40 articles for analysis. After reading the abstracts, 20 were discarded because they did not fully address the inclusion criteria, so 20 studies remained for full reading of the articles. After careful reading, 14 articles were discarded because they did not present relevant data for this study. Therefore, 6 articles remained for the final sample (Figure 1).

Figure 1

Flowchart for identifying the databases and selecting the articles



Source: prepared by the authors based on the Prisma model.

3 RESULTS

The final sample resulted in 6 articles that were analyzed in terms of database, study title, author and abstract, which can be seen in Figure 2.

Figure 2

Database, study title, author, and abstract selected from the scientific literature between 2019 and 2025

DATABASES	STUDY TITLE	AUTHOR AND CITATION	STUDY SUMMARY

Scielo Brazil	Digital inclusion and Internet use among older adults in Brazil: a cross- sectional study	Jamylle Diniz; Andréa Carvalho Araújo Moreira; Iane Ximenes Teixeira; Samir Gabriel Vasconcelos Azevedo; Cibelly Aliny Siqueira Lima Freitas; Iasmin Cunha Maranguape. Maranguape *et al.* (2020)	To describe the profile of Brazilian elderly people who use the internet, the means of access and the purpose of this use, and to verify the existence of an association between sociodemographic variables and those related to the use of the internet.
Lilacs	Cyberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos?	James Rincón; Santiago Castiblanco; Andrés Quijano; Juan Urquijo; Yuliana Pregonero. Rincón *et al.* (2022)	In 2019, it obtained 23,917 complaints for crimes considered computer-related. Of this total, about 13,242 corresponded to 55% for the crime of computer theft, followed by access to the computer system with 3,492, complaints with 14.6%, in addition to the violation of personal data of 3,178 which characterized 13.29%.
Latindex	Cybercrime – challenges for the law	Flavio Mirã de Souza Nogueira; Loreci Gottschalk Nolasco. Walnut and Nolasco (2022)	He pointed out that the embezzlement of electronic fraud has seen a notable growth in several Brazilian states and even in European nations, as an illustration, in the State of São Paulo it was raised to 256% and, in Minas Gerais, it registered an increase of 50% in 2022.
PubMed	The influence of Cybercrime and legal awareness on the behavior of university of Jordan students.	Ismael Alhadidi; Aman Nweiran b; Ghofran Hilal. Alhadid *et al*. (2024)	A population comprising a random sample of

			2,000 students enrolled at the University of Jordan. The objective was to implement effective strategies to increase students' legal awareness of cybercrime, to mitigate their involvement. In addition, he also brought the information that there are 1 million crimes on the internet annually in Jordan.
Scielo	Análisis espacial del ciberfraude al comercio electrónico: consideraciones en agenda política Tamaulipeca.	Rosa Amelia Domínguez Arteaga; Rodrigo Vera Vázquez. Domínguez Arteaga and Vera Vázquez (2022)	The goal is to review the techniques used by cybercriminals and determine the spatial distribution of cyberfraud against e-commerce in Tamaulipas. The techniques used by cybercriminals were mainly the use of social media to steal passwords. Methodologically, an analysis of calls to the Federal Police for cybercrimes was carried out from 2018 to 2019, applying the location coefficient. The result: a concentration of connections in Nayarit, Jalisco and Chihuahua. Tamaulipas has been identified as a prone location for this cybercrime in the national context.
PlumX Metrics	Balance of the main cybercrimes that		Data collection through the Public

	occurred in the municipality of Belém/PA in the period from 2018 to 2020	Luciana Corrêa e Silva; Diego de Azevedo Gomes. Silva and Azevedo (2023)	Security Secretariat of the State of Pará - SEGUP and in the estimated time from 2018 to July 2022. The cybercrimes that stood out the most in her study were: computer device invasion and embezzlement with about 6,496 and 4,490, respectively. The virtual embezzlement was highlighted for the female sex and emphasized that women are more vulnerable in the digital environment.

Source: prepared by the authors, 2025.

4 DISCUSSION

The research by the authors Maranguape et al. (2020) revealed that, among frequent users of the digital environment, women accounted for more than half (n= 200; 52.08%) of the recorded occurrences. In a convergent way, Silva and Azevedo (2023) confirmed that women are more often victims of cybercrimes, reinforcing the vulnerability of this group.

In a study carried out in Colombia by Rincón et al. (2022), they analyzed the period from 2010 to 2020. In 2019, (n= 13,242; 55%) of the complaints related to computer crimes in the country referred to computer theft, mostly concentrated in Bogotá - which can be attributed to both the greater exposure of the population and the greater accessibility to reporting services.

The study by Nogueira and Nolasco (2022) also indicated a notable growth in embezzlement and electronic fraud in several Brazilian states, for example, in São Paulo, the increase was 256%, while in Minas Gerais, there was a 50% increase in records of this type of crime in 2022.

The results of the study coincide with the trend observed at the international level of growth in cybercrime. An example is the study carried out in Jordan, which showed an increase in these crimes in the last decade - from 1,320 cases in 2013 to 16,027 in 2022 (Alhadidi et al., 2024). This scenario reveals a global escalation of digital infractions, which requires integrated prevention, education and repression actions, adapted to different sociocultural contexts.

The study by Domínguez Arteaga and Vera Vázquez (2022) pointed out that the phishing technique is one of the main means used by cybercriminals in Mexico, corresponding to more than 80% of cases in Mexico City. The theft of social network passwords was also highlighted, registering more than 160 cases. In addition, the information presented by the Federal Police, with regard to cybercrimes, was highlighted mainly in the State of Mexico, Mexico City and Guanajuato of the actions of cybercriminals being (n = 493), (n = 425) and (n = 263), respectively; in addition to Tamaulipas being in 13th place with 94 records (DOMÍNGUEZ ARTEAGA; VERA VÁZQUEZ, 2022).

Studies such as that of Silva and Azevedo (2023) point out that business hours concentrate a greater volume of electronic fraud attempts, given the greater interaction with financial services and shopping platforms. On the other hand, the crimes of defamation and threat, even because they had fewer records, were more frequent on weekends, especially on Saturdays and Sundays, and especially the night shift.

The elderly, in particular, are more affected by virtual scams, especially those based on the phishing technique, due to factors such as cognitive vulnerability, social isolation, and difficulties with the use of technologies. In the studies by authors Maranguape et al. (2020), Brazilian older people have autonomy and independence in the use of technologies in cyberspace for more than two hours in their daily lives. These records suggest that the elderly population has become a preferred target in electronic embezzlement scams, possibly due to less familiarity with digital environments, greater reliance on virtual contacts and, in many cases, access to pensions or fixed income.

5 CONCLUSION

This integrative review evidenced the significant growth and diversification of cybercrimes, both in the national and international context, highlighting modalities such as phishing, credential theft, embezzlement, and electronic fraud. The data analyzed show that women and the elderly are among the most vulnerable groups, either due to greater exposure to the digital environment, or due to sociocultural and technological factors.

It was found that cybercriminals' strategies vary according to the location, the profile of the victims and the available resources, adapting quickly to new opportunities and technologies. This criminal flexibility reinforces the need for integrated public policies, investments in digital education, and strengthening of reporting and repression mechanisms.

The convergence between studies from different countries indicates that cybercrime is a global and dynamic phenomenon, requiring equally dynamic and coordinated responses. In this scenario, international information sharing and cooperation between governments, security institutions, and civil society become essential to prevent the impacts of these crimes.

Finally, the use of integrative review allowed for the effective gathering and systematization of the scientific evidence available in both national and international databases, in addition to contributing to future research and public policy managers.

REFERENCES

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of cybercrime and legal awareness on the behavior of University of Jordan students. Heliyon, 10(12), e32371. https://doi.org/10.1016/j.heliyon.2024.e32371

Arsawati, N. J., Darma, M. W., & Antari, P. E. D. (2021). A criminological outlook of cyber crimes in sexual violence against children in Indonesian laws. International Journal of Criminology and Sociology, 10, 219–223. https://doi.org/10.6000/1929-4409.2021.10.26

Clough, J. (2010). Principles of cybercrime. New York, NY: Cambridge University Press.

Domínguez Arteaga, R. A., & Vera Vázquez, R. (2022). Análisis espacial del ciberfraude al comercio electrónico: Consideraciones en agenda política Tamaulipeca. Podium, (41), 21–40. https://revistas.uees.edu.ec/index.php/Podium/article/view/745

Instituto Brasileiro de Geografia e Estatística (IBGE). (2021). Pesquisa Nacional por Amostra de Domicílios: 90% dos lares brasileiros já tem acesso à internet no Brasil, aponta pesquisa. https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-internet-no-brasil-aponta-pesquisa

Lorenzo, L. P., & Scaravelli, G. P. (2021). 5 cibercrimes e a legislação brasileira. Diálogos e Interfaces do Direito-FAG, 4(1), 104–122.

Maia, E. (2024, May 3). Ataques hackers aumentam 8,8% no Brasil e país segue como 2° mais atacado do mundo. CNN Brasil. https://www.cnnbrasil.com.br/nacional/ataques-hackers-aumentam-88-no-brasil-e-pais-segue-como-2o-mais-atacado-do-mundo/

Maranguape, I. C., Moreira, A., Samir, V., Diniz, J., Teixeira, I., Lima, C., & Carvalho, A. (2020). Inclusão digital e o uso da internet pela pessoa idosa no Brasil: Estudo transversal. Revista Brasileira de Enfermagem, 3.

Mendes, K. D. da S., Silveira, R. C. C. P., & Galvão, C. M. (2008). Revisão integrativa: Método de pesquisa para a incorporação de evidências na saúde e na enfermagem. Texto & Contexto – Enfermagem, 17(4), 758–764. https://doi.org/10.1590/S0104-07072008000400018

McQuade III, S. C. (2006). Understanding and managing cybercrime. Boston, MA: Pearson.

Nogueira, F., & Nolasco, L. G. (2022). Crimes cibernéticos - Desafios para o direito. Revista Jurídica Direito, Sociedade e Justiça, 9(13), 133–140.

Pinheiro, P. P. (2021). Direito digital (7th ed.). São Paulo, Brazil: Saraiva.

Rincón, J., Quijano, A., Castiblanco, S., Urquijo, J., & Pregonero, Y. (2022). Ciberdelincuencia en Colombia: ¿Qué tan eficiente ha sido la Ley de Delitos Informáticos? Revista Criminalidad, 64(3), 95–116. https://doi.org/10.47741/17943108.368

Silva, L. C., & Azevedo, D. G. de. (2022). Balanço dos principais crimes cibernéticos ocorridos no município de Belém/PA no período de 2018 a 2020. Research, Society and Development, 11(1). https://doi.org/10.33448/rsd-v11i1.25214

Souza, D. da P. (2021). Proteção de dados e o processo penal: Desafios e parâmetros da cadeia de custódia da prova digital (Undergraduate thesis, Universidade de Brasília, Brasília, Brazil). https://bdm.unb.br/handle/10483/28900

Souza, M. T., Silva, M. D. da, & Carvalho, R. de. (2010). Revisão integrativa: O que é e como fazer. Einstein, 8(1), 102–106. https://doi.org/10.1590/S1679-45082010RW1134

Trend Micro. (2024). Relatório da Trend Micro coloca o Brasil entre os cinco países mais atacados por ransomware em abril. https://dciber.org/relatorio-da-trend-micro-coloca-o-brasil-entre-os-cinco-paises-mais-atacados-por-ransomware-em-abril/

Turgal, J. (2023, May). Cyber warfare lessons from the Russia-Ukraine conflict. Dark Reading. https://tinyurl.com/licoes-russia-ucrania