


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

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

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

 <https://doi.org/10.56238/arev7n8-257>

Data de submissão: 28/07/2025

Data de publicação: 28/08/2025

Daniel Braga da Silva

Mestre em Perícias Forenses pelo Programa de Pós-Graduação em Perícias Forenses
Instituição: Universidade de Pernambuco (UPE)
E-mail: danielbraga.silva@upe.br
Lattes: <http://lattes.cnpq.br/2495010715300669>
Orcid: <https://orcid.org/0009-0009-4844-3138>

Adriana Conrado de Almeida

Doutora em Saúde Materno Infantil
Instituição: Instituto de Medicina Integral Professor Fernando Figueira (IMIP - Conceito CAPES 5)
E-mail: adriana.almeida@upe.br
Lattes: <http://lattes.cnpq.br/3892527052352252>
Orcid: <https://orcid.org/0000-0001-6141-0458>

Carmen Silvia Arraes de Alencar Valença

Doutoranda em Perícias Forenses
Instituição: Universidade de Pernambuco
E-mail: carmen.valenca@upe.br
Lattes: <http://lattes.cnpq.br/8764643264668578>
Orcid: <https://orcid.org/0000-0002-6430-9707>

Clarissa Alencar de Macau Furtado

Estudante de Medicina
Instituição: Faculdade de Ciências Médicas Afya - Jaboatão dos Guararapes
E-mail: clarissamacau@gmail.com
Lattes: <http://lattes.cnpq.br/0589563486101637>
ORCID: <https://orcid.org/0009-0004-3070-767X>

Histephane Maria Bezerra de Vasconcelos

Mestranda de Perícias Forenses pelo Programa de Pós-Graduação em Perícias Forenses
Instituição: Universidade de Pernambuco (UPE)
E-mail: hmbvlife@hotmail.com
Lattes: <http://lattes.cnpq.br/468803671225616>
Orcid: <https://orcid.org/0009-0007-3081-6691>

Luina Alencar Trajano

Mestra em Perícias Forenses pelo Programa de Pós-Graduação em Perícias Forenses
Instituição: Universidade de Pernambuco (UPE)
E-mail: luinalencar@gmail.com
Lattes: <http://lattes.cnpq.br/0463740047240711>
ORCID: <https://orcid.org/0009-0005-6244-8163>

Marta Victor de Araujo

Mestranda de Perícias Forenses pelo Programa de Pós-Graduação em Perícias Forenses
Instituição: Universidade de Pernambuco (UPE)
E-mail: marta.victoraraujo@upe.br
Lattes: <http://lattes.cnpq.br/2929512073508593>
Orcid: <https://orcid.org/0009-0003-2484-892X>

Betise Mery Alencar Sousa Macau Furtado

Doutora em Ciências
Instituição: Fundação Oswaldo Cruz
E-mail: betisemery@gmail.com
Lattes: <http://lattes.cnpq.br/4682659587643054>
ORCID: <https://orcid.org/0000-0001-6344-8257>

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.

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. 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.

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. Interdisciplinarietà.

1 INTRODUÇÃO

A internet foi criada em meados de 1960 como um recurso militar durante o contexto da Guerra Fria. No Brasil, sua chegada ocorreu no final da década de 1980. Tornou-se pública e comercializada entre 1994 e 1995. Segundo a Pesquisa Nacional por Amostra de Domicílios, em 2021, aproximadamente de 90% dos lares brasileiros tinham acesso à internet e apontado pelo Instituto Brasileiro de Geografia e Estatística (IBGE, 2021).

É notória a importância da internet na vida das pessoas em todo o mundo, uma vez que é uma ferramenta facilitadora no cotidiano, além de permitir a divulgação de notícias livremente por meio da rede mundial de computadores (WEB). Semelhante ao mundo real, surge neste ambiente, práticas ilícitas, semelhantes às capituladas no Código Penal, como exemplo, os crimes contra a honra, a dignidade da pessoa humana e sexual, preconceito racial, ideias supremacistas, fraudes eletrônicas, dentre outros (PINHEIRO, 2021). Estes crimes passam a ser denominados de cibercrimes, entendidos como sendo infrações cometidas no mundo virtual, mostrando assim a transformação da forma delitiva tradicional para o digital (ARSAWATI ET AL., 2021). Historicamente, o primeiro delito auxiliado pelo computador foi em 1958, nos Estados Unidos da América, em que um funcionário do banco de Minneapolis, alterou programas de um banco para depositar pequenas quantidades de centavos resultantes de milhões de transações financeiras e, no ano de 1966, foi registrada a primeira condenação por uma corte federal americana pela manipulação de dados bancários (MCQUADE, 2006).

São amplamente reconhecidos os aspectos positivos dos meios eletrônicos e da comunicação virtual, pois facilitam a aproximação entre as pessoas por meio da conexão digital, além de favorecerem o desempenho profissional, especialmente com a popularização do trabalho remoto (home office). Por conseguinte, muitos criminosos virtuais ou cibercriminosos agem sob a falsa premissa de que o ambiente virtual ou ciberespaço, está isento de leis ou regras, acreditando que podem cometer delitos sem enfrentar consequências legais. Este ambiente é compreendido como um ambiente em constante transformação, marcado por múltiplas formas de interação social e tecnológica (SOUZA, 2021).

No ciberespaço, há uma democratização quanto ao reconhecimento do perfil criminológico denominado de haters, hackers e cibercriminosos que comumente operam os ciberataques, quando esses ataques são relacionados aos sistemas de informação, ou quando são utilizados computadores ou a internet como meio para a ação criminosa ou cibercrime (LORENZO; SCARAVELLI, 2021). Os cibercriminosos estão acompanhando o avanço da sociedade digital hiperconectada na rede, com impactos estratégicos por meio da manipulação de programas, utilizando-se das falhas dos meios de proteção virtual para as práticas ilícitas (TURGAL, 2023).

Estima-se que o Brasil sofreu 328.326 ciberataques no primeiro semestre de 2023 e, no segundo semestre do mesmo ano, cerca de 357.422 ataques com destaque nas telecomunicações sem fio (MAIA, 2024). Na ótica do panorama mundial, o Brasil ocupou o quinto lugar a partir de dados de abril de 2024 dentre os países que sofreram ciberataques através dos ransomware, uma forma de sequestrar informações digitais das vítimas. A Tailândia aparece em primeiro lugar (44,1%), seguida pelos Estados Unidos (24,3%), Turquia (8,8%), Alemanha (2,7%) e Brasil com (1,8%) (TREND MICRO, 2024).

Diante do exposto e com o intuito de contribuir com a literatura acadêmica, o presente estudo teve como 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, a fim de compreender e aprofundar os conhecimentos, além de oferecer subsídios empíricos para a formulação de políticas públicas voltadas à prevenção e repressão de crimes cibernéticos.

2 METODOLOGIA

Foi utilizado neste estudo uma revisão integrativa da literatura a fim de analisar e sistematizar a produção acadêmica existente sobre o tema, tendo em vista que este tipo de estudo assegura o rigor metodológico e uma análise crítica consistente das publicações selecionadas (SOUZA; SILVA; CARVALHO, 2020). A busca na literatura correu entre novembro de 2024 a 30 de junho de 2025. Para a seleção das publicações nas bases de dados foram utilizadas as palavras-chaves: cibercrimes, cybercrimes, crimes cibernéticos e crimes na internet, nas bases de dados Scopus, PubMed, Medline, Lilacs, Scielo, Scielo Brasil, Latindex e PlumX Metrics referente ao período de 2019 a 2025.

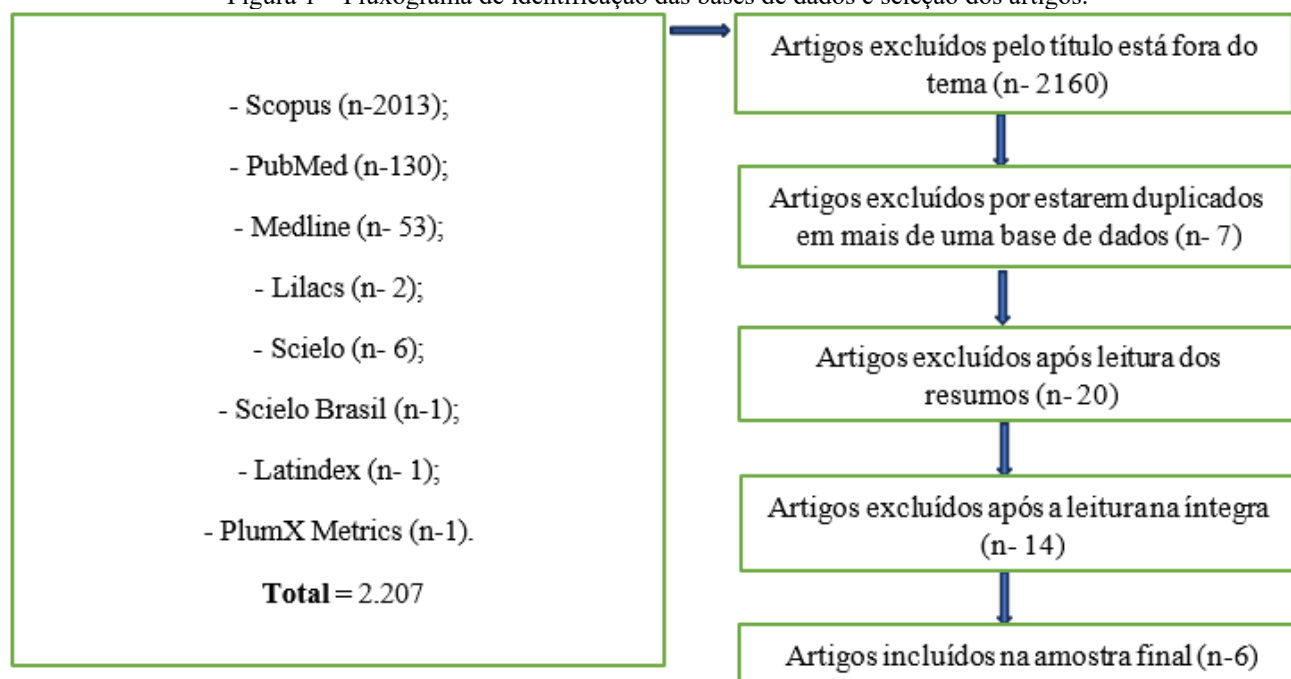
Há uma dualidade quanto ao uso da palavra cibercrime com i e com y. A nomenclatura com y para cybercrime, foi a priori defendida por Susman e Heuston (1995), mas efetivamente usada em 1997 quando tratou do relatório de comissão presidencial, no qual foi reunida para estudos relacionado à proteção de infraestrutura crítica (MCQUADE, 2006). Nesta pesquisa, será utilizada a terminologia cibercrime com i, defendida por Jonathan Clough e ordenada na Convenção de Budapeste (CLOUGH, 2010).

Foram considerados como critérios de inclusão artigos publicados no período estudado; com acesso gratuito; em qualquer idioma. Foram excluídos artigos duplicados em mais de uma base de dados; revisões de literatura, carta ao editor, teses, dissertações, capítulos de livro e documentos oficiais sobre o tema. Para maior amplitude da busca foi utilizado o operador booleano AND.

Do total de 2.207 (dois mil duzentos e sete) estudos identificados inicialmente, 2.160 foram excluídos por não se encontrarem dentro do tema após a leitura dos títulos. Restaram 47, destes 7 foram

excluídos por se encontrarem duplicados, em mais de uma base de dados, restando 40 artigos para análise. Após a leitura dos resumos, 20 foram descartados por não abordarem de forma completa os critérios de inclusão, assim restaram 20 estudos para leitura completa dos artigos. Após a leitura criteriosa, foram descartados 14 artigos por não apresentarem dados relevantes para este estudo. Portanto, 6 artigos restaram para amostra final (Figura 1).

Figura 1 – Fluxograma de identificação das bases de dados e seleção dos artigos.



Fonte: elaborado pelos autores com base no modelo Prisma.

3 RESULTADOS

A amostra final resultou em 6 artigos que foram analisados quanto a base de dados, título do estudo, autor e resumo, no qual pode ser observado na Figura 2.

Figura 2 – Base de dados, título do estudo, autor e resumo selecionado na literatura científica entre 2019 e 2025.

BASES DE DADOS	TÍTULO DO ESTUDO	AUTOR E CITAÇÃO	RESUMO DO ESTUDO
Scielo Brasil	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 <i>et al.</i> (2020)	Descrever o perfil de pessoas idosas brasileiras que utilizam internet, o meio de acesso e a finalidade desse uso, e verificar a existência de associação entre variáveis sociodemográficas e aquelas relacionadas ao uso da internet.

Lilacs	Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos?	James Rincón; Santiago Castiblanco; Andrés Quijano; Juan Urquijo; Yuliana Pregonero. Rincón <i>et al.</i> (2022)	No ano de 2019, obteve 23.917 denúncias para os crimes considerados informáticos. Desse total, cerca de 13.242 correspondeu 55% para o delito furto informático, na sequência, acesso no sistema informático com 3.492, reclamações com 14,6%, além da violação de dados pessoais de 3.178 que caracterizou 13,29%.
Latindex	Crimes cibernéticos – desafios para o direito	Flavio Mirã de Souza Nogueira; Loreci Gottschalk Nolasco. Nogueira e Nolasco (2022)	Sinalizou que o estelionato fraude eletrônica houve um crescimento notável em vários Estados brasileiros e até em nações europeias, a modo de ilustração, no Estado de São Paulo foi elevado para 256% e, em Minas Gerais, registrou ampliação de 50% no ano de 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 <i>et al.</i> (2024)	Uma população que compreende uma amostra aleatória de 2.000 alunos matriculados na Universidade da Jordânia. Objetivou-se implementar estratégias eficazes para aumentar a conscientização legal dos alunos em relação ao crime cibernético, para mitigar seu envolvimento. Outrossim, trouxe também a informação que acontece 1 milhão de crimes na internet anualmente na Jordânia.
Scielo	Análisis espacial del ciberfraude al comercio electrónico: consideraciones en agenda política Tamaulipeca.	Rosa Amelia Domínguez Arteaga; Rodrigo Vera Vázquez. Domínguez Arteaga e Vera Vázquez (2022)	O objetivo é revisar as técnicas usadas pelos criminosos cibernéticos e determinar a distribuição espacial da fraude cibernética contra o comércio eletrônico em Tamaulipas. As técnicas usadas pelos criminosos cibernéticos foram principalmente o uso de mídias sociais para roubar senhas. Metodologicamente, foi realizada uma análise das ligações para a Polícia Federal por crimes cibernéticos de 2018 a 2019, aplicando o coeficiente de localização. Resultado: uma concentração de ligações em Nayarit, Jalisco e Chihuahua. Tamaulipas foi identificada como um local propenso para esse crime cibernético no contexto nacional.

PlumX Metrics	Balanço dos principais crimes cibernéticos ocorridos no município de Belém/PA no período de 2018 a 2020	Luciana Corrêa e Silva; Diego de Azevedo Gomes. Silva e Azevedo (2023)	Coleta dos dados através da Secretaria de Segurança Pública do Estado do Pará - SEGUP e no tempo estimado de 2018 até julho de 2022. Os crimes cibernéticos que tiveram mais destaques no estudo dela foram: a invasão de dispositivo informático e estelionato com cerca de 6.496 e 4.490, respectivamente. O estelionato virtual foi destaque para o sexo feminino e enfatizou que as mulheres são mais vulneráveis em meio digital.
---------------	---	--	--

Fonte: elaborado pelos autores, 2025.

4 DISCUSSÃO

A pesquisa dos autores Maranguape et al. (2020), revelou que, entre os usuários frequentes do meio digital, as mulheres representaram mais da metade (n= 200; 52,08%) das ocorrências registradas. De forma convergente, Silva e Azevedo (2023) confirmaram que mulheres são mais frequentemente vítimas de crimes cibernéticos, reforçando a vulnerabilidade desse grupo.

Em estudo realizado na Colômbia por Rincón et al. (2022), analisou o período de 2010 a 2020. Em 2019, (n= 13.242; 55%) das denúncias relacionadas a crimes informáticos no país referiam-se ao furto informático, concentrando-se majoritariamente em Bogotá - o que pode ser atribuído tanto à maior exposição da população quanto à maior acessibilidade aos serviços de denúncia.

O estudo de Nogueira e Nolasco (2022) também indicou um crescimento notável no estelionato e na fraude eletrônica em vários estados brasileiros, a título de exemplo, em São Paulo, o aumento foi de 256%, enquanto em Minas Gerais, houve uma ampliação de 50% nos registros desse tipo de crime no ano de 2022.

Os resultados do estudo coincidem com a tendência observada em nível internacional de crescimento dos crimes cibernéticos. Um exemplo é o estudo realizado na Jordânia, que evidenciou um aumento desses delitos na última década - passando de 1.320 casos em 2013 para 16.027 em 2022 (Alhadidi et al., 2024). Esse cenário revela uma escalada global das infrações digitais, que exige ações integradas de prevenção, educação e repressão, adaptadas a diferentes contextos socioculturais.

O estudo de Domínguez Arteaga e Vera Vázquez (2022) apontou que a técnica phishing é um dos principais meios utilizados por cibercriminosos no México, correspondendo a mais de 80% dos casos na Cidade do México. Também se destacou o roubo de senhas de redes sociais registrando mais de 160 casos. Ademais, as informações apresentadas pela Polícia Federal, no que se rereferiu aos crimes cibernéticos, tiveram como destaques principalmente no Estado do México, cidade do México e Guanajuato das ações dos cibercriminosos sendo (n= 493), (n= 425) e (n= 263), respectivamente;

além que Tamaulipas ficou em 13º lugar com 94 registros (DOMÍNGUEZ ARTEAGA; VERA VÁZQUEZ, 2022).

Estudos como o de Silva e Azevedo (2023) apontam que o horário comercial concentra maior volume de tentativas de fraudes eletrônicas, dada a maior interação com serviços financeiros e plataformas de compras. Por outro lado, os crimes de difamação e ameaça, ainporque com menor registros, apresentaram maior frequência nos finais de semana, sobretudo aos sábados e domingos, e com destaque para o turno da noite.

Os idosos, em particular, são mais afetados por golpes virtuais, sobretudo os baseados na técnica de phishing, em razão de fatores como vulnerabilidade cognitiva, isolamento social e dificuldades com o uso de tecnologias. Nos estudos dos autores Maranguape et al. (2020), pessoas idosas brasileiras têm autonomia e indepência no uso das tecnologias no ciberespaço por mais de duas horas no dia a dia. Esses registros sugerem que a população idosa tem se tornado um alvo preferencial em golpes de estelionato eletrônico, possivelmente em razão de menor familiaridade com ambientes digitais, maior confiança em contatos virtuais e, em muitos casos, acesso a aposentadorias ou rendimentos fixos.

5 CONCLUSÃO

A presente revisão integrativa evidenciou o crescimento expressivo e a diversificação dos cibercrimes, tanto no contexto nacional quanto internacional, destacando modalidades como phishing, roubo de credenciais, estelionato e fraude eletrônica. Os dados analisados mostram que mulheres e idosos figuram entre os grupos mais vulneráveis, seja por maior exposição ao meio digital, seja por fatores socioculturais e tecnológicos.

Verificou-se que as estratégias dos cibercriminosos variam conforme a localidade, o perfil das vítimas e os recursos disponíveis, adaptando-se rapidamente a novas oportunidades e tecnologias. Essa flexibilidade criminosa reforça a necessidade de políticas públicas integradas, investimentos em educação digital e fortalecimento dos mecanismos de denúncia e repressão.

A convergência entre estudos de diferentes países indica que a criminalidade cibernética é um fenômeno global e dinâmico, exigindo respostas igualmente dinâmicas e coordenadas. Nesse cenário, o compartilhamento internacional de informações e a cooperação entre governos, instituições de segurança e sociedade civil tornam-se fundamentais para prevenir os impactos desses delitos.

Por fim, a utilização da revisão integrativa permitiu reunir e sistematizar de forma eficaz as evidências científicas disponíveis nas bases de dados tanto nacional quanto internacional, além de contribuir para futuras pesquisas e gestores de políticas públicas.

REFERÊNCIAS

- ALHADIDI, Ismaeel; NWEIRAN, Aman; HILAL, Ghofran. The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. *Heliyon*, v. 10, n. 12, e32371, 2024. Disponível em: <https://doi.org/10.1016/j.heliyon.2024.e32371>. Acesso em: 13 jul. 2024.
- ARSAWATI, Nyoman Juwita; DARMA, Made Wirya; ANTARI, Putu Eva Ditayani. A Criminological Outlook of Cyber Crimes in Sexual Violence Against Children in Indonesian Laws. *Internacional Journal of Criminology and Sociology*, v. 10, p. 219–223, 2021. Disponível em: <https://doi.org/10.6000/1929-4409.2021.10.26>. Acesso em: 13 jul. 2024.
- CLOUGH, Jonathan. *Principles of Cybercrime*. New York: Cambridge University Press, 2010.
- DOMÍNGUEZ ARTEAGA, Rosa Amelia; VERA VÁZQUEZ, Rodrigo. Análisis espacial del ciberfraude al comercio electrónico: consideraciones en agenda política Tamaulipeca. *Podium*, n. 41, p. 21–40, 2022. Disponível em: <https://revistas.uees.edu.ec/index.php/Podium/article/view/745>. Acesso em: 13 jul. 2024.
- INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). Pesquisa Nacional por Amostra de Domicílios: 90% dos lares brasileiros já tem acesso à internet no Brasil, aponta pesquisa. Rio de Janeiro: IBGE, 2021. Disponível em: <https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-internet-no-brasil-aponta-pesquisa>. Acesso em: 4 jun. 2025.
- LORENZO, Larissa Papandreus; SCARAVELLI, Gabriela Paiva. 5 Cibercrimes e a legislação brasileira. *Diálogos e Interfaces do Direito-FAG*, v. 4, n. 1, p. 104-122, 2021.
- MAIA, Eljonas. Ataques hackers aumentam 8,8% no Brasil e país segue como 2º mais atacado do mundo. *CNN Brasil*, 3 maio 2024. Disponível em: <https://www.cnnbrasil.com.br/nacional/ataques-hackers-aumentam-88-no-brasil-e-pais-segue-como-2o-mais-atacado-do-mundo/>. Acesso em: 5 jun. 2025.
- MARANGUAPE, Iasmin Cunha; MOREIRA, Andrea; SAMIR, Vasconcelos; DINIZ, Janylle; TEIXEIRA, Iane; LIMA, Cibelly; CARVALHO, Andréa. Inclusão digital e o uso da internet pela pessoa idosa no Brasil: estudo transversal. *Revista Brasileira de Enfermagem*, v. 3, 2020.
- MENDES, Katia Denise da Silva; SILVEIRA, Rosane C. C. P.; GALVÃO, Cristina Maria. Revisão integrativa: método de pesquisa para a incorporação de evidências na saúde e na enfermagem. *Texto & Contexto – Enfermagem*, v. 17, n. 4, p. 758-764, 2008.
- NOGUEIRA, Flavio; NOLASCO, Loreci Gottschalk. Crimes cibernéticos - desafios para o direito. *Revista Jurídica Direito, Sociedade e Justiça*, v. 9, n. 13, p. 133–140, 2022.
- MCQUADE III, Samuel C. *Understanding and managing cybercrime*. Boston: Pearson, 2006.
- PINHEIRO, Patrícia Peck. *Direito digital*. 7. ed. São Paulo: Saraiva, 2021.

RINCÓN, Jaime; QUIJANO, Andrés; CASTIBLANCO, Santiago; URQUIJO, Juan; PREGONERO, Yuliana. Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos? *Revista Criminalidad*, v. 64, n. 3, p. 95-116, 2022. Disponível em: <https://doi.org/10.47741/17943108.368>. Acesso em: 13 jul. 2024.

SILVA, Luciana Corrêa; AZEVEDO, Diego Gomes de. Balanço dos principais crimes cibernéticos ocorridos no município de Belém/PA no período de 2018 a 2020. *Research, Society and Development*, v. 11, n. 1, 2022. Disponível em: <https://doi.org/10.33448/rsd-v11i1.25214>. Acesso em: 15 jan. 2025.

SOUZA, Déborah da Paz. Proteção de dados e o processo penal: desafios e parâmetros da cadeia de custódia da prova digital. 2021. 64 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade de Brasília, Brasília, 2021. Disponível em: <https://bdm.unb.br/handle/10483/28900>. Acesso em: 8 jun. 2025.

SOUZA, Marcela Tavares; SILVA, Michelly Dias da; CARVALHO, Raquel de. Revisão integrativa: o que é e como fazer. *Einstein*, v. 8, n. 1, p. 102-106, 2010.

TREND MICRO. Relatório da Trend Micro coloca o Brasil entre os cinco países mais atacados por ransomware em abril. São Paulo, 2024. Disponível em: <https://dciber.org/relatorio-da-trend-micro-coloca-o-brasil-entre-os-cinco-paises-mais-atacados-por-ransomware-em-abril/>. Acesso em: 7 jul. 2025.

TURGAL, James. Cyber Warfare Lessons From the Russia-Ukraine Conflict. *Dark Reading*, maio 2023. Disponível em: <https://tinyurl.com/licoes-russia-ucrania>. Acesso em: 10 jun. 2025.