UniFacema
Centro Universitário de Ciências e Tecnologia do Maranhão
ISSN: 2447-2301

REVISÃO / REVIEW / REVISIÓN

CYBERCRIMES, INVASIONS, AND FRAUDS ON SOCIAL MEDIA: REFLECTIONS ON BRAZILIAN CRIMINAL LAW AND THE ROLE OF DIGITAL FORENSIC EXPERTISE

CIBERCRIMES, INVASÕES E FRAUDES EM REDES SOCIAIS: REFLEXÕES SOBRE O DIREITO PENAL BRASILEIRO E O PAPEL DA PERÍCIA FORENSE DIGITAL

CIBERCRÍMENES, INVASIONES Y FRAUDES EN REDES SOCIALES: REFLEXIONES SOBRE EL DERECHO PENAL BRASILEÑO Y EL PAPEL DE LA PERICIA FORENSE DIGITAL

Rivaldo Brito Serra[1]

Gentil Reis da Cunha Santos Filho[2]

Emerson Farias de Souza[3]

Letícia Maysa da Costa Machado Matos de Carvalho[4]

DESCRIPTORS
Social media. Cybercrimes. Penal Law. Digital Forensics.

DESCRITORES
Cibercrimes. Direito Penal. Perícia Digital.

DESCRIPTORES
Cibercrímenes. Derecho Penal. Pericia Digital

ABSTRACT
Introduction: The research addressed the issues of cybercrimes, intrusions, and fraud on social networks, highlighting Brazilian Criminal Law and the role of digital forensic expertise in investigating these crimes. **Objectives:** The research aimed to examine the obstacles encountered by the Brazilian legal system in dealing with cybercrimes and to examine the importance of digital forensics in this process. **Methods:** Through literature review, documentary analysis, and data collection, Brazilian legislation related to cybercrimes, such as the Carolina Dieckmann Law (Law n.º 12.737/12), and the role of computer forensic expertise in enforcing these laws were investigated. **Results:** The findings revealed a significant increase in cyber attacks in Brazil, demonstrating the diversity and sophistication of criminal practices in the digital environment. Despite legislative advancements and the role of digital forensics, challenges were identified, such as the lack of professional training and the rapid evolution of technologies. **Conclusion:** The research emphasized the importance of protecting the personal data of Brazilian citizens and the need to enhance prevention and investigation strategies to effectively combat cybercrimes. The relevance of awareness and training of involved professionals was highlighted, as well as the urgency of effective measures to ensure a safe and reliable online environment.

RESUMO
Introdução: A pesquisa abordou a problemática dos cibercrimes, invasões e fraudes em redes sociais, destacando o Direito Penal brasileiro e o papel da perícia forense digital na investigação desses crimes. **Objetivos:** a pesquisa visou examinar os obstáculos encontrados pelo sistema legal do Brasil ao lidar com os crimes cibernéticos e examinar a importância da perícia digital nesse procedimento. **Métodos:** Por meio de revisão bibliográfica, análise documental e de dados, foram investigadas a legislação brasileira relacionada aos crimes cibernéticos, como a Lei Carolina Dieckmann (Lei n.º 12.737/12), e a atuação da perícia forense computacional na aplicação dessas leis. **Resultados:** Os resultados revelaram um aumento significativo nos ataques cibernéticos no Brasil, evidenciando a diversidade e sofisticação das práticas criminosas no ambiente digital. Apesar dos avanços legislativos e da atuação da perícia digital, foram identificados desafios, como a falta de capacitação de profissionais e a rápida evolução das tecnologias. **Conclusão:** A pesquisa ressalta a importância da proteção dos dados pessoais dos cidadãos brasileiros e a necessidade de aprimorar as estratégias de prevenção e investigação para enfrentar de forma eficaz os cibercrimes. Destacou-se a relevância da conscientização e capacitação dos profissionais envolvidos, bem como a urgência de medidas eficazes para garantir um ambiente online seguro e confiável.

RESUMEN
Introducción: La investigación abordó la problemática de los cibercrímenes, invasiones y fraudes en redes sociales, destacando el Derecho Penal brasileño y el papel de la pericia forense digital en la investigación de estos crímenes. **Objetivos:** La investigación tuvo como objetivo examinar los obstáculos que enfrenta el sistema legal brasileño al lidiar con los delitos cibernéticos y evaluar la importancia de la pericia digital en este proceso. **Métodos:** A través de una revisión bibliográfica, análisis documental y de datos, se investigó la legislación brasileña relacionada con los delitos cibernéticos, como la Ley Carolina Dieckmann (Ley N.º 12.737/12), y el papel de la pericia forense computacional en la aplicación de estas leyes. **Resultados:** Los resultados revelaron un aumento significativo en los ataques cibernéticos en Brasil, destacando la diversidad y sofisticación de las prácticas criminales en el entorno digital. A pesar de los avances legislativos y la actuación de la pericia digital, se identificaron desafíos, como la falta de capacitación de profesionales y la rápida evolución de las tecnologías. **Conclusión:** La investigación resalta la importancia de proteger los datos personales de los ciudadanos brasileños y la necesidad de mejorar las estrategias de prevención e investigación para enfrentar eficazmente los cibercrímenes. Se destacó la relevancia de la concienciación y capacitación de los profesionales involucrados, así como la urgencia de medidas eficaces para garantizar un entorno en línea seguro y confiable

[1] Graduando do Curso de Bacharelado em Direito pelo Centro Universitário de Ciencias e Tecnologia do Mararnhão. E-mail: rivaldoserr@gmail.com
[2] Especialista em Direito Penal e Porcesso Penal. Docente do Curso de Bacharelado em Direito pelo Centro Universitário de Ciencias e Tecnologia do Mararnhão. E-mail: gentilfilho9@gmail.com
[3] Doutor em Políticas Públicas. Mestre em Educação. Docente do Curso de Bacharelado em Direito pelo Centro Universitário de Ciencias e Tecnologia do Mararnhão.
[4] Mestre em Teoria Literária. Docente do Curso de Bacharelado em Direito pelo Centro Universitário de Ciencias e Tecnologia do Mararnhão.

1. INTRODUÇÃO

A era digital trouxe consigo uma revolução nas interações sociais, com as redes sociais se tornando plataformas predominantes para comunicação e compartilhamento de informações. No entanto, esse ambiente virtual também se tornou um espaço propício para a prática de crimes cibernéticos, que atentam contra a privacidade, a segurança e os direitos dos usuários.

A Constituição Federal de 1988, em seu artigo 5º, inciso X, assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, bem como o direito à indenização pelo dano material ou moral decorrente de sua violação. No entanto, a crescente incidência de crimes cibernéticos nas redes sociais desafia diretamente esses princípios fundamentais, com criminosos utilizando técnicas sofisticadas para acessar, manipular ou destruir dados digitais alheios.

É imperativo que o Estado atue de forma decisiva para garantir a efetividade desses direitos, através da prevenção e punição dos crimes cibernéticos. No entanto, o enfrentamento desse fenômeno pelo Direito Penal brasileiro é permeado por uma série de desafios, que requerem uma abordagem multidisciplinar e coordenada, com destaque para o papel crucial desempenhado pela perícia digital.

Embora o Brasil tenha avançado na legislação relacionada aos crimes cibernéticos, com a promulgação de leis como a Lei dos Crimes Cibernéticos n.º 12.737/2012 e a recente Lei n.º 14.155/2021, que alterou o Código Penal e o Código de Processo Penal, persistem lacunas e deficiências no combate a esses delitos.

Diante desse cenário desafiador, este artigo propõe uma análise aprofundada sobre a eficácia do Direito Penal brasileiro no enfrentamento dos cibercrimes, invasões e fraudes em redes sociais. Para isso, destaca-se a importância da perícia digital como um instrumento essencial para a apuração e a solução desses crimes.

Desse modo, o presente artigo levanta os seguintes questionamentos: Como o Direito Penal brasileiro enfrenta os cibercrimes nas redes sociais, como as invasões e fraudes? Qual é o papel da perícia digital nesse processo?

Diante do que foi exposto acima, este estudo tem como finalidade desenvolver uma compreensão mais profunda dos crimes cibernéticos nas redes sociais, um fenômeno que atinge milhões de brasileiros e coloca em risco a privacidade, a segurança e a dignidade dos usuários da internet. A seleção deste tema foi motivada pela sua notável importância nos âmbitos social, jurídico e acadêmico. Justifica-se pela complexidade e natureza dinâmica do assunto, que demandam uma atualização contínua e a salvaguarda dos direitos e interesses dos indivíduos nas redes sociais.

2. METODOLOGIA

Trata-se de uma pesquisa de revisão bibliográfica, análise documental e de dados com uma perspectiva dedutiva, visando explorar criticamente o conhecimento existente sobre o tema em questão. Para tanto, utilizaram-se fontes acadêmico-doutrinárias, legislação brasileira, periódicos científicos, monografias e artigos científicos, obtidos por meio de diversas bases de dados, incluindo o Google Acadêmico e Scielo.

Para a progressão deste trabalho foi

imprescindível o levantamento bibliográfico e de literatura acerca dos seguintes temas relacionados à pesquisa: Direito Penal, Direito Digital e Perícia Digital.

Além da revisão bibliográfica, a análise das leis pertinentes também desempenhou um papel crucial no desenvolvimento deste artigo. Especificamente, foram analisadas a Lei dos Crimes Cibernéticos n.º 12.737 de 2012, Lei n.º 12.965 de 2014, Lei n.º 13.709 de 2018 e a Lei n.º 14.155 de 2021, fornecendo uma base legal para a discussão dos aspectos jurídicos relacionados aos cibercrimes, invasões e fraudes em redes sociais.

O período de agosto a novembro de 2023 foi dedicado às fases de revisão bibliográfica, análise documental e análise de dados. Este recorte temporal permitiu uma abordagem sistemática e detalhada do tema, garantindo a qualidade e a profundidade da pesquisa realizada.

3. RESULTADOS

Os resultados obtidos na pesquisa sobre cibercrimes, invasões e fraudes em redes sociais revelaram um panorama preocupante, evidenciando um aumento significativo nos ataques cibernéticos, especialmente após a retomada das atividades econômicas pós-pandemia. A análise dos exemplos apresentados, como os ataques de phishing e as invasões de contas, ressaltou a diversidade e sofisticação das práticas criminosas no ambiente digital, destacando a urgência de medidas eficazes para enfrentar essas ameaças.

No decorrer da pesquisa, foram exploradas e investigadas a legislação brasileira relacionada aos crimes cibernéticos, com destaque para a importância da Lei Carolina Dieckmann (Lei n.º 12.737/12), o Marco Civil da Internet (Lei n.º 12.965/2014) e da Lei Geral de Proteção de Dados (Lei n.º 13.709/2018). Além disso, foi enfatizado o papel crucial desempenhado pela perícia forense computacional na aplicação dessas leis, fornecendo evidências técnicas e forenses essenciais para apoiar a investigação e o processamento legal dos casos.

Essas leis representam avanços significativos ao estabelecer penalidades para crimes digitais e definir regras de competência. No entanto, desafios significativos foram identificados pelo sistema jurídico brasileiro na investigação e punição dos crimes cibernéticos. A rápida evolução da tecnologia e das táticas de ataque cibernético exige uma resposta igualmente dinâmica por parte das autoridades e dos profissionais envolvidos.

A pesquisa enfatizou a importância da capacitação contínua dos profissionais envolvidos na prevenção e investigação de crimes cibernéticos. A adaptação às novas ameaças e a compreensão das nuances legais são fundamentais para garantir uma resposta eficaz e adaptativa diante das complexidades do cenário digital.

Eles examinam cuidadosamente o conteúdo das mensagens de phishing, os endereços de e-mail dos remetentes, os endereços dos sites falsos e outros indicadores de fraude. Além disso, realizam análises forenses em computadores e dispositivos comprometidos para identificar possíveis vetores de ataque e rastrear a origem das campanhas de phishing.

Ao fornecer análises técnicas detalhadas e relatórios periciais precisos, os peritos digitais ajudam as autoridades a entender a extensão dos ataques de phishing, identificar possíveis vulnerabilidades de segurança e desenvolver estratégias eficazes de prevenção e resposta a esses tipos de crimes cibernéticos. Assim, a perícia digital desempenha um papel crucial na proteção dos usuários online e na promoção da segurança cibernética em geral.

Os resultados do estudo também destacaram a necessidade de cooperação entre diferentes entidades, incluindo órgãos governamentais, instituições de ensino, empresas privadas e organizações da sociedade civil. A colaboração multidisciplinar é essencial para desenvolver estratégias abrangentes de prevenção e combate aos crimes cibernéticos. A proteção dos dados pessoais dos cidadãos brasileiros e a promoção da segurança digital emergem como questões de interesse público, demandando ações coordenadas e efetivas por parte das autoridades e profissionais envolvidos no combate aos cibercrimes, invasões e fraudes em redes sociais.

Além disso, o estudo identificou lacunas na capacidade investigativa e técnica das autoridades responsáveis pela aplicação da lei no contexto dos crimes cibernéticos. A crescente atenção dada aos crimes cibernéticos no contexto jurídico brasileiro reflete a necessidade premente de adaptação do ordenamento jurídico às dinâmicas do ambiente digital. Investimentos adicionais em treinamento, tecnologia e infraestrutura são necessários para fortalecer as capacidades de combate a esses delitos.

Diante do exposto, os resultados obtidos nesta pesquisa não apenas contribuem para o entendimento das nuances e desafios dos crimes cibernéticos, mas também ressaltam a importância da legislação, da perícia digital e do investimento em capacitação profissional. A pesquisa reforça a importância de estar preparado para enfrentar as ameaças emergentes e garantir um ambiente online seguro e confiável para todos os usuários, em meio ao avanço contínuo na era digital.

4. DISCUSSÃO

4.1. A Revolução Digital e o Direito Digital Brasileiro

O advento da internet marcou um ponto crucial na evolução da sociedade contemporânea, desencadeando mudanças profundas na maneira como nos comunicamos, interagimos e realizamos nossas atividades diárias. O avanço tecnológico na comunicação sempre buscou estabelecer uma Aldeia Global, onde o acesso à informação ocorre de forma simultânea em todo o mundo. A internet, com sua capacidade de conectar pessoas globalmente, revolucionou não apenas os fluxos de informação, mas também as esferas do comércio e da cultura (Pinheiro, 2021, p. 23).

Essa revolução digital concretizou a visão de um mundo interconectado, transformando-o numa sociedade digital, onde cada interação e transação reflete a integração e a interdependência global. No entanto, essa transformação não veio sem desafios, especialmente no campo jurídico, onde as leis tradicionais e o trabalho forense muitas vezes se mostram inadequados ou insuficientes para lidar com as complexidades do mundo digital.

Apesar dos privilégios que a internet oferece aos seus usuários, ela também se tornou um terreno fértil para atividades criminosas. Conforme destacado por Lorenzo e Scaravelli (2021, p. 4), os crimes virtuais, que surgiram e evoluíram juntamente com essa expansão tecnológica, estão em constante evolução, visando prejudicar principalmente os usuários.

A evolução histórica dos crimes cibernéticos remonta aos primórdios da computação e da conectividade digital. Segundo Silva (2021, p. 7), os crimes virtuais tiveram origem na Guerra Fria, na década de 1960, com os primeiros casos de manipulação, sabotagem e espionagem utilizando a tecnologia emergente. Com a internet surgindo em 1969, inicialmente para uso militar, houve um avanço significativo nesse campo. Na década de 1980, esses delitos se intensificaram, abrangendo manipulações bancárias, pornografia infantil e pirataria de programas.

Essa tendência alarmante evidencia uma

consequência direta do progresso e da disseminação da tecnologia. Como argumenta Patrícia Peck (2021, p. 24):

> Se entendermos que a Internet é um lugar, então muitas questões do Direito devem ser redesenhadas, uma vez que o território ou jurisdição deveria ser a própria Internet. Se entendermos que a Internet é um meio, então voltamos a ter de resolver a questão da territorialidade para aplicação da norma, já havendo como referência a atuação do Direito Internacional.

O direito digital, portanto, surge como uma resposta essencial à necessidade de regulamentação e proteção dos direitos no ambiente online, englobando uma vasta gama de questões, desde a proteção da privacidade dos dados até a responsabilidade civil e penal por atividades na internet.

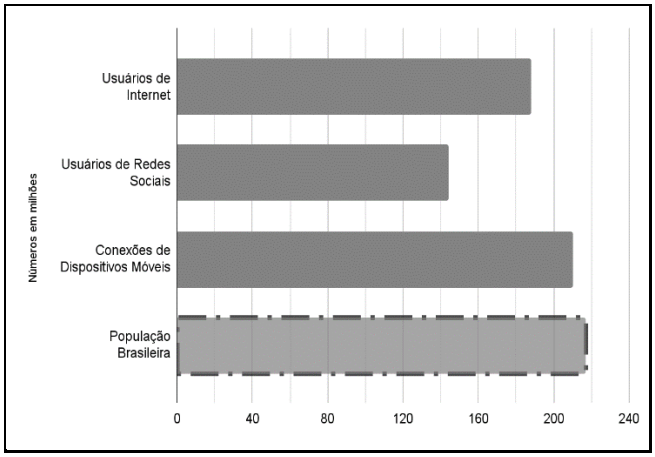
Pinheiro (2021, p. 24) sugere que não devemos falar em Direito de Internet, mas sim em um único Direito Digital cujo grande desafio é estar preparado para o desconhecido, seja aplicando antigas ou novas normas, mas com a capacidade de interpretar a realidade social e adequar a solução ao caso concreto na mesma velocidade das mudanças da sociedade.

No Brasil, inicialmente, a abordagem do tema foi predominantemente voltada para questões de direito penal, culminando na edição da Lei n.º 7.646/87 em 1987. Esta lei, como destacado por Bispo e Binto (2023, p. 359), procura principalmente a proteção da propriedade intelectual relacionada a softwares e sua comercialização no território nacional.

Segundo Silva (2021, p. 8), o Brasil teve acesso às redes internacionais para pesquisa em 1991, mas foi apenas em 1995 que o acesso para consumo se expandiu, trazendo consigo o impacto imediato dos crimes virtuais. A consciência sobre a gravidade desses crimes começou a se solidificar em 1996, quando sites ligados ao governo foram invadidos por criminosos.

Atualmente, as redes sociais têm um papel crucial na sociedade brasileira, apresentando uma parcela significativa entre a população. Um levantamento realizado pela DataReportal (2024, online) em janeiro de 2024 revelou que o Brasil contava com 187,9 milhões de usuários de internet, o que corresponde a 86,6% da população total. Além disso, o país possuía 144,0 milhões de usuários ativos em mídias sociais, representando 66,3% da população total.

Gráfico 1 - Dados do relatório Digital Brasil 2024 sobre usuários, dispositivos e população em 2024



Fonte: DataReportal, (2024).

O Gráfico 1 revela que, é evidente que as mídias sociais ainda desempenham um papel significativo na vida digital dos brasileiros, com uma parcela considerável da população sendo ativa nessas plataformas.

4.1.2 Perícia Forense Digital

Em paralelo ao desenvolvimento das matérias, leis e regulamentações para enfrentar os crimes cibernéticos, a perícia forense digital emerge como uma peça-chave para a eficácia do direito penal no enfrentamento desses delitos.

Nesse escopo, Oliveira, Santiago, Costa (2023, p. 3983) definem a perícia forense computacional como o processo de coleta, análise e preservação de evidências digitais, sendo um meio de prova utilizado no âmbito das investigações e processos judiciais. Esses especialistas, denominados peritos, são profissionais qualificados e imparciais, possuindo domínio técnico e científico em suas respectivas áreas.

Vilela, Giraldi e Vilela (2023, p. 4) enfatizam

em sua pesquisa que o escopo da perícia forense digital transcende os delitos estritamente tecnológicos. A perícia se estende ao uso de equipamentos e tecnologias pertencentes aos suspeitos para rastrear provas, validando a ocorrência de um delito, que pode ser tanto cibernético quanto tradicional. Esta abordagem ampla é crucial para a eficácia da perícia forense em um espectro diversificado de casos criminais.

Sua importância reside na capacidade de proporcionar clareza e objetividade aos processos judiciais. Ao introduzir conhecimentos técnicos e científicos no tribunal, a prova pericial auxilia os agentes públicos na compreensão de aspectos complexos e específicos, visando à melhor aplicação das normas jurídicas e à proteção das empresas e da sociedade em geral (Cadilhac apud Oliveira, Santiago, Costa, 2023, p. 3985).

4.2. Crimes Cibernéticos e a Perícia Forense Digital

4.2.1 Conceito e Classificações do Cibercrime

Primordialmente, faz-se necessária a delimitação conceitual do termo "cibercrime", uma vez que este abrange uma ampla gama de práticas criminosas ocorridas no ambiente digital. Desde crimes tradicionais adaptados para o meio virtual, como fraudes, roubos e extorsões, até formas de crime inteiramente novas possibilitadas pela tecnologia, como o phishing e o malware, o universo dos cibercrimes é vasto e multifacetado.

A literatura acadêmica apresenta diversas terminologias empregadas em estudos sobre o crime cibernético, o que reflete a complexidade e a dinâmica desses delitos. Para Teixeira (2022, p. 223) , o crime de informática abrange não apenas a internet, mas todo o sistema informático. Portanto, o crime praticado por meio da internet é uma forma específica do crime de informática, o qual possui uma área de abrangência mais ampla.

Por sua vez, Zambonato (2022, p. 15) define o crime cibernético como qualquer conduta típica, antijurídica e culpável que utiliza recursos tecnológicos como meio para a prática delituosa, podendo ser cometida tanto contra quanto por meio de dispositivos e seus sistemas. Para Vieira (2020, p. 16),

> Os crimes virtuais são aqueles cometidos via 'internet' e podem ser enquadrados no nosso código penal, onde terá punições de acordo com cada caso. Tais crimes começaram a aparecer, pois, o aumento de usuários na 'internet' foi crescendo cada vez mais, como vimos no número de acesso do facebook, com esse aumento desses usuários alguns criminosos viram que tinham a oportunidade de tirar algum proveito dessa situação.

Essas variações refletem as diversas perspectivas disciplinares, jurídicas e tecnológicas envolvidas na compreensão dos crimes cibernéticos. A constante evolução da tecnologia e das táticas de ataques cibernéticos têm desafiado as estruturas de segurança e aplicação da lei, exigindo respostas igualmente dinâmicas e adaptativas para enfrentar essa ameaça em constante transformação.

Quanto à classificação, os crimes cibernéticos são divididos pela vertente doutrinária em próprios e impróprios. Essa sistematização é amplamente utilizada pelos estudiosos do tema devido à sua simplicidade e abrangência (Zambonato, 2022, p. 15).

Os crimes próprios são aqueles que exigem o uso de tecnologia da informação e comunicação como meio para sua consumação, como nos casos de invasões de sistemas e ataques de negação de serviço. Teixeira (2022, p. 224) leciona:

> Esta modalidade que é a pura criminalidade informática. São também conhecidos como crimes de informática próprios, praticados por meio da infor-mática; sem ela são impossíveis a execução e a consumação do delito. São tipos penais relativamente novos, pois surgiram a partir do desenvolvimento e expansão da informática, sendo a informática o bem penalmente tutelado.

Por outro lado, segundo o mesmo autor, os crimes impróprios são as infrações já previstas penalmente, que não se enquadram como crimes de informática. São atos que envolvem a utilização da tecnologia da informação, ou seja, todos os delitos que se utilizam dessa tecnologia para sua execução. Exemplos incluem o estelionato virtual, a invasão de contas bancárias online e as fraudes em transações eletrônicas.

4.2.2 Etapas e Evidências da Perícia Forense Digital

A perícia forense digital compreende um procedimento meticuloso e sistemático, abarcando diversas fases. De acordo com Pereira e Oliveira (apud Franck e Ferreira, 2023, p. 119), as principais etapas desse processo são a coleta e catalogação dos dados, exame, a análise forense e a apresentação do laudo pericial.

Segundo Vilela, Giraldi e Vilela (2023, p. 5), após a obtenção das evidências pelo perito, inicia-se um processo de análise detalhada e perícia técnica. Durante essa fase, são executadas várias operações críticas, incluindo a restauração de dados excluídos, a procura por arquivos em dispositivos de grande capacidade de armazenamento, a decifração e análise dos dados recuperados, o manejo de sistemas de criptografia para prevenir acessos indevidos e a extração segura de informações, preservando a integridade dos dados, como é o caso na quebra de senhas.

Na prática, isso significa que os peritos forenses digitais devem ser capazes de combinar suas habilidades técnicas com uma compreensão sólida dos procedimentos legais e dos requisitos de evidências em processos judiciais. Eles precisam não apenas extrair e analisar dados de dispositivos digitais, mas também apresentar suas descobertas de maneira clara e objetiva em relatórios periciais que possam ser compreendidos por advogados, juízes e júris.

A atribuição de responsabilidade por delitos cibernéticos demanda a verificação de diversos elementos, como a identificação do autor do ato, a presença de intencionalidade, o emprego de recursos tecnológicos e a invasão não autorizada de informações. Dessa forma, torna-se imprescindível a execução de perícias técnicas em equipamentos que armazenam dados para coletar evidências que sustentem a acusação (Oliveira, et al, 2023, p. 3985).

Principalmente, em investigações de crimes virtuais, devido à facilidade de adulteração de dados, as provas exigirão análises técnicas rigorosas para serem admitidas em juízo, assegurando a validade e integridade das evidências.

Para Duarte (2022, p. 24),

> A computação forense é um tipo de perícia qualificada pela inspeção cientifica e sistemática em computadores, modo que através da coleta de provas digitais, busca chegar a conclusões sobre o fato investigado, devendo ser feita uma reconstituição dos eventos encontrados, possibilitando determinar se a aparelho eletrônico analisado foi utilizado para a realização ou não de condutas ilícitas.

É importante destacar que, conforme a legislação brasileira sobre delitos digitais, todos os recursos legítimos são admissíveis na coleta de evidências, incluindo a obtenção de documentos, depoimentos e a realização de perícias técnicas.

Essa abordagem integrada permite que os peritos forenses digitais desempenhem um papel eficaz na investigação e resolução de casos judiciais envolvendo evidências digitais. Eles não apenas fornecem uma análise técnica das evidências digitais, mas também ajudam a traduzir essas informações em termos legais compreensíveis, ajudando assim a garantir a justiça e a integridade do processo judicial.

4.3. Crimes Cibernéticos e Perícia Forense Digital na Legislação Brasileira

No que tange à definição e abordagem dos crimes cibernéticos, a legislação brasileira busca abarcar uma variedade de práticas criminosas online. O estelionato virtual em foco nesta pesquisa, é

tipificado como crime no Código Penal Brasileiro, Título II, Capítulo VI, artigo 171, § 2º-A, dispõe o seguinte:

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo (BRASIL, 2021).

Para Cleber Masson (2024, p. 567), o estelionato qualificado, apresentado nos termos da Lei 14.155/2021, é um crime de alto potencial ofensivo, no qual a fraude é um elemento essencial para sua caracterização. Em outras palavras, o estelionato não pode existir sem que haja fraude. O autor também esclarece que:

Nessa qualificadora, a fraude é praticada com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. Esse meio de execução especial é que diferencia a figura qualificada do estelionato catalogado no art. 171, caput, do Código Penal, no qual a fraude é genérica (ou residual), ou seja, consiste em qualquer artifício, ardil ou outro meio fraudulento diverso dos elencados pelo § 2.º-A do art. 171 do Código Penal (Masson, 2024, p. 567).

Por sua vez, Silva e Carvalho (2022, p. 55), disciplinam:

> Não obstante, com a novatio legis in pejus, incluindo o §2º - A no artigo 171 do Código Penal (BRASIL, 2021), essa conduta se torna qualificada, ou seja, no caso da dosimetria da pena, o juiz já inicia a primeira fase, ainda que com todas as circunstâncias judiciais favoráveis do artigo 59 do Código Penal (BRASIL 1940), com uma pena mínima de 4 (quatro) anos, sendo que o agente que pratica o delito do caput do artigo 171 desse código (BRASIL 1940) inicia sua primeira fase (considerando as circunstâncias judiciais favoráveis) com uma pena mínima de 1 (um) ano.

Conforme apontado por Miranda (2023, p. 12), tanto o estelionato tradicional quanto sua versão qualificada, o estelionato digital, compartilham semelhanças no que diz respeito à fraude, engano e obtenção de vantagem de maneira ilícita. No entanto, as diferenças entre essas modalidades residem principalmente nos meios e métodos empregados.

Enquanto o estelionato tradicional opera por meio de transações físicas, como cheques sem fundo e cartões clonados, o estelionato digital é predominantemente realizado em ambiente virtual, por meio de golpes via e-mails, ligações telefônicas e mensagens de aplicativos de conversas, se intensificou durante a pandemia da COVID-19, à medida que o distanciamento social levou as pessoas a permanecerem em suas residências (Masson, 2024, p. 567).

A disseminação de fraudes online, como esquemas de pirâmide, venda de produtos falsificados, divulgação de serviços fraudulentos, como os golpes que envolvem o sistema Pagamento Instantâneo Brasileiro (PIX), também se enquadram nessa categoria, representando uma ameaça constante para os usuários, os consumidores e a economia digital.

Entretanto, Pedrosa e Coltro (2022, p. 108) destacam que, conforme as circunstâncias do caso, a tipificação legal de uma determinada conduta pode ser alterada.

Sabe-se que as circunstâncias de caso podem alterar a tipificação legal de um determinado ato, como por exemplo se no caso em questão houver algum tipo de violência ou constrangimento com o fito de obter a vantagem, o que poderia levar a conduta a ser entendida como uma extorsão (Art. 158). Todavia, nos casos mais corriqueiros, muitas vezes a conduta tem as mesmas características e são imputadas de maneiras

diversas, seja como estelionato (Art. 171 do CP) ou outras vezes como furto mediante fraude (Art. 155, § 4º, inciso II do CP) (Pedrosa e Coltro 2022, p. 108).

Destarte, os indivíduos que praticam crimes envolvendo transações via Pix podem ser processados por estelionato ou furto mediante fraude, com possíveis penas de dois a oito anos de reclusão. Adicionalmente, podem ser enquadrados em crimes como associação criminosa, esquemas de pirâmide financeira e lavagem de dinheiro.

Além disso, práticas criminosas diversas, como a disseminação de vírus e a fraude eletrônica, são abordadas por diferentes dispositivos, leis e regulamentações no Brasil. A exemplo, os casos de phishing, nos quais os indivíduos são enganados para fornecer informações confidenciais, como senhas e números de cartão de crédito, são frequentes nesse contexto. Vieira (2020, p. 26), em seu livro sobre Prevenção em Crimes Cibernéticos, define o phishing como conversas ou mensagens falsas contendo endereços fraudulentos. O principal objetivo dessa prática é "pescar" informações pessoais e confidenciais da vítima, com o intuito de lesá-la.

Os peritos digitais utilizam técnicas especializadas para analisar os dados coletados de mensagens de phishing, sites fraudulentos e registros de atividades de rede. A partir da análise dessas comunicações, eles podem identificar esquemas de fraude em sistemas bancários, onde os dados de cartões bancários e de crédito das vítimas são obtidos. Tal fraude geralmente começa com o envio em massa de e-mails, atingindo centenas de milhares ou até mesmo milhões de destinatários em diferentes estados brasileiros (Silva Filho, 2018, p. 61).

Segundo um relatório divulgado em 2023 pela Kaspersky, uma empresa global especializada em cibersegurança e privacidade digital, o Brasil testemunhou um aumento significativo de cinco vezes no número de bloqueios de phishing nos últimos 12 meses. O relatório revelou um total de 134 milhões de tentativas de ataque registradas durante esse período. Conforme análise dos especialistas da empresa, credita-se tal aumento a retomada de atividades econômicas pós-pandemia e o surgimento de ferramentas usando a inteligência artificial (Kaspersky, 2023).

Outro exemplo é a invasão de contas, na qual os criminosos obtêm acesso não autorizado a contas de endereço eletrônico, redes sociais ou serviços bancários online, muitas vezes resultando em roubo de identidade e prejuízos financeiros significativos para as vítimas.

De acordo com Teixeira (2022, p. 228), é frequente a divulgação de notícias sobre invasões de computadores e servidores por hackers e crackers, visando diversos propósitos. Essa conduta criminosa consiste na invasão de dispositivos informáticos alheios, independentemente de estarem conectados ou não à rede de computadores. Essa invasão ocorre por meio da violação indevida de mecanismos de segurança, com o intuito de obter, adulterar ou destruir dados, ou informações sem a autorização expressa, ou tácita, do titular do dispositivo. Além disso, é relevante salientar que a instalação de vulnerabilidades visando obter vantagem ilícita também faz parte desse quadro.

A legislação brasileira aborda essa prática criminosa no artigo 154-A do Código Penal, instituído pela Lei n. 12.737/2012, não apenas tipifica o crime de invasão de dispositivo informático, mas também estabelece penalidades para a divulgação ou comercialização dos dados obtidos. A pena pode variar de três meses a um ano de prisão, além de multa, se a invasão resultar em obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido (Brasil, 2021).

Salienta-se que esse dispositivo legal define o crime de invasão de dispositivo informático, o qual, juntamente com outras infrações à inviolabilidade dos segredos, compõe os denominados crimes contra a

liberdade individual.

A compreensão das nuances e particularidades de cada categoria de crime cibernético é crucial para a prevenção, investigação e punição adequadas. Para tal, a integração com perícia digital não se limita à investigação de casos após sua ocorrência, mas também se estende à prevenção e à adaptação contínua às novas ameaças.

Como observado por Martins (2020, p. 02), com a crescente utilização da internet pela maioria da população global, criminosos rapidamente adaptaram suas estratégias, executando fraudes eletrônicas e capitalizando sobre o medo e a ansiedade gerados pela pandemia e pelo isolamento social subsequente. Essa rápida adaptação ao ambiente digital reflete a agilidade com que atividades ilícitas podem evoluir em resposta a mudanças sociais e tecnológicas.

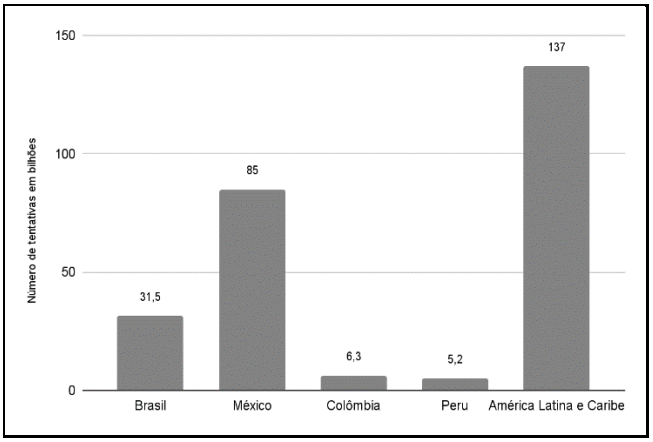
Apesar dos esforços legislativos, o sistema jurídico brasileiro enfrenta desafios significativos na investigação e punição dos crimes cibernéticos. Como destacado por, Lima e Soares (apud Frank e Ferreira, 2023, p. 123),

As leis tiveram que se modernizar com o avanço tecnológico. Com surgimento da informática e sua ampla e rápida disposição à sociedade e passou a exigir também com rapidez, soluções que o Direito não estava preparado para resolver. Diante desse contexto, a necessidade social aparenta estar desprovida da tutela do Direito e a busca ansiosa por regular a matéria pode provocar a criação de leis excessivas e desnecessárias.

Portanto, é fundamental que profissionais jurídicos, órgãos de aplicação da lei e especialistas em segurança digital estejam familiarizados com os diferentes tipos de crimes cibernéticos e suas características distintivas.

Não obstante, a análise conduzida pela empresa de cibersegurança Fortinet, revela que, no primeiro semestre de 2022, o Brasil enfrentou um considerável aumento nas tentativas de ataques cibernéticos, totalizando 31,5 bilhões, representando um crescimento de 94% em relação ao período homólogo. Esse estudo, posiciona o Brasil como o segundo país mais afetado da América Latina, atrás apenas do México (FortiGuard Labs, 2022). O Gráfico 2, mostra o número de tentativas de ataques cibernéticos no primeiro semestre de 2022 para alguns países latino-americanos, incluindo o total para a América Latina e Caribe.

Gráfico 2 - Tentativas de ataques cibernéticos no primeiro semestre de 2022



Fonte: Elaborado pelo autor, (2024).

No contexto jurídico brasileiro, os crimes cibernéticos têm recebido crescente atenção, refletindo a urgência de adaptação do ordenamento jurídico às dinâmicas do ambiente digital. Zambonato (2022, p. 30) conclui que a ausência de tipificação de crimes cibernéticos perdurou por décadas, sendo somente em 2012 que houve uma regulamentação. Essa demora na criação da lei prejudicou significativamente a sociedade brasileira, que ficou desprotegida contra as novas modalidades de crimes, e também afetou negativamente a comunidade internacional, que clamava há muito tempo por uma medida eficaz para enfrentar essas ameaças.

A promulgação da Lei n.º 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, marcou um importante avanço na legislação brasileira em relação aos delitos informáticos. Embora grande parte de seus dispositivos represente uma especialização de quesitos já presentes no código penal ou em outras normas, essa

lei foi pioneira ao estabelecer medidas específicas de proteção no meio digital, especialmente no que diz respeito à punibilidade de crimes complexos como a invasão de dispositivos de informática (Tremel e Nascimento, apud Araujo e Couto, 2023, p.8).

Quanto às alterações feitas, pela Lei n.º 14.155/2021 Zambonato destaca:

No dia 27 de maio de 2021, após um intervalo de nove anos, a Lei nº 14.155/2021 foi sancionada para realizar alterações na Lei nº 12.737/12 (Lei Carolina Dieckman), que disciplina o crime de invasão de dispositivo informático, previsto no art. 154-A do CP, de modo a modificar a sua redação e tornar mais severa a sua pena. Da mesma forma, a legislação em comento trouxe ao ordenamento jurídico modalidades específicas do crime de furto e estelionato quando praticados por meio eletrônico, além de definir regras de competência para este último (Zambonato, 2022, p. 36).

Conforme mencionado, esta legislação representou um avanço significativo ao estabelecer penalidades para a invasão de dispositivos informáticos alheios, bem como para a obtenção, transferência ou divulgação não autorizada de dados pessoais.

Dessa forma, a compreensão que se extrai é que a perícia forense computacional desempenha um papel crucial na aplicação da Lei Carolina Dieckmann (Lei n.º 12.737/2012) e suas alterações subsequentes, como a Lei n.º 14.155/2021. A perícia forense computacional é responsável por investigar e coletar evidências digitais relacionadas a crimes cibernéticos, incluindo invasão de dispositivos informáticos e obtenção não autorizada de dados pessoais.

A partir desse marco, outras legislações relevantes foram promulgadas para regular o ambiente digital no Brasil. O Marco Civil da Internet (MCI), instituído pela Lei n.º 12.965/2014, é outra peça importante nesse quebra-cabeça jurídico digital. Para Teixeira (2022, p. 41) trata-se de uma lei principiológica, pois estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, assegurando a liberdade de expressão, a privacidade dos usuários e a neutralidade da rede, além de tratar de questões como a responsabilidade dos provedores de serviços online.

Lima (2022, p. 14) ressalta que a garantia de neutralidade, um dos princípios basilares do MCI (Lei n.º 12.965/2014) assegura o tratamento isonômico dos pacotes de dados, conforme regulamentado no artigo 9º do mesmo diploma. Isso não apenas preserva a internet como um canal de comunicação livre, mas também protege a liberdade de escolha dos usuários e fomenta a livre concorrência.

No entanto, apesar dos esforços regulatórios como o MCI, a proteção da privacidade dos usuários tem enfrentado desafios crescentes. Com o aumento da proliferação de informações pessoais online, como observado por Zambonato (2022, p. 23), a preservação de evidências em casos de infrações online tornou-se uma tarefa complexa para os processos de investigação criminal.

Essa complexidade é ressaltada ainda mais pela ausência de regulamentações específicas sobre a retenção e o uso dos dados dos usuários. Pinheiro (2021, p. 33), aponta que antes da implementação do Marco Civil, caso um usuário encerrasse sua relação com o serviço, seus dados poderiam ser retidos pela empresa por tempo indeterminado, sem restrições quanto ao uso para diversos propósitos.

Não obstante, a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), Lei n.º 13.709/2018, representou um passo fundamental para a proteção da privacidade e dos dados pessoais dos cidadãos brasileiros. Para Zambonato (2022, p. 34) A LGPD em adição ao MCI (Lei n.º 12.965/2014), foram estabelecidas diretrizes mais específicas referentes ao tratamento de dados e à privacidade dos cidadãos, abrangendo também aqueles originados do ambiente digital.

Essa interação entre o MCI (Lei n.º 12.965/2014), a LGPD (Lei n.º 13.709/2018) e outras regulamentações pertinentes, evidencia uma

preocupação contínua com a proteção dos direitos dos usuários no ambiente digital, proporcionando um arcabouço jurídico mais robusto para enfrentar os desafios emergentes relacionados à privacidade e à segurança dos dados pessoais.

Segundo Bispo e Binto (2023, p. 364),

> O objetivo da LGPD é disciplinar e regulamentar o uso dos dados pessoais mantidos por empresas e órgãos governamentais, afim que se evitem abuso contra aqueles que confiarem a suas informações pessoais sobre a sua guarda. Todas as organizações públicas ou privadas que detém dados pessoais de pessoas naturais, com o objetivo de oferecer ou ter que prestar serviços, estão sujeitos ao regramento da LGPD.

No entanto, mesmo com esses avanços regulatórios, o cenário de ameaças cibernéticas avançadas continua evoluindo, como destaca o relatório de previsões de ameaças de 2024 do FortiGuard Labs (2024). O uso crescente de Inteligência Artificial nos ataques representa um desafio significativo para a segurança digital.

Diante deste panorama, torna-se imperativo o investimento na capacitação contínua dos profissionais, bem como na atualização constante das técnicas e tecnologias empregadas. Isso garante uma resposta efetiva e adaptativa às complexidades que evoluem continuamente no cenário digital.

Silva (2023, p. 18) ressalta a importância desse investimento para assegurar a eficácia e a adaptabilidade diante das mudanças do ambiente digital. Ele destaca que o aperfeiçoamento contínuo dos profissionais é crucial para manter a relevância e a eficácia das estratégias utilizadas, promovendo uma abordagem cada vez mais qualificada e eficiente frente às transformações do cenário digital.

Além disso, é essencial promover uma cultura organizacional que valorize a segurança cibernética em todos os níveis, desde a alta administração até os funcionários de base. Isso inclui a conscientização sobre práticas seguras de navegação na internet, o uso adequado de dispositivos e redes corporativas e a importância de relatar quaisquer incidentes de segurança imediatamente.

Em suma, a segurança cibernética é um desafio em constante evolução que exige uma abordagem multifacetada e colaborativa. Somente com investimentos contínuos em capacitação, tecnologia e cooperação, podemos garantir a proteção eficaz dos dados pessoais e a preservação da integridade do ambiente digital.

5. CONCLUSÃO

Ao longo desta pesquisa, exploramos os desafios e complexidades dos crimes cibernéticos, destacando a importância da legislação e da perícia digital na resposta a essas ameaças. Diante da extensão do tema e da quantidade de informações apresentadas, é essencial retomar brevemente a problemática central que norteou nosso estudo.

Os resultados obtidos revelam um panorama preocupante, com um aumento significativo nos ataques cibernéticos, especialmente após a retomada das atividades econômicas pós-pandemia. Os exemplos apresentados, como os ataques de phishing e as invasões de contas, evidenciam a diversidade e sofisticação das práticas criminosas no ambiente digital, destacando a urgência de medidas eficazes para enfrentar essas ameaças.

Em resposta à questão de como o Direito Penal brasileiro pode enfrentar os cibercrimes, invasões e fraudes em redes sociais de forma eficaz e adequada, investigamos a legislação brasileira relacionada aos

crimes cibernéticos, ressaltando a importância da Lei Carolina Dieckmann (Lei n.º 12.737/2012) e da Lei Geral de Proteção de Dados (Lei n.º 13.709/2018). Além disso, exploramos o papel crucial da perícia forense computacional na aplicação dessas leis, fornecendo evidências técnicas e forenses para apoiar a investigação e o processamento legal dos casos.

Apesar dos avanços legislativos e da atuação da perícia digital, ainda existem desafios a serem superados. A falta de capacitação de profissionais, a escassez de recursos e a rápida evolução das tecnologias representam obstáculos para a eficácia no combate aos crimes cibernéticos. Nesse sentido, sugerem-se investimentos em treinamento e atualização constante, bem como o aprimoramento das estratégias de prevenção e investigação

Iniciativas como o Instituto Nacional de Combate ao Cibercrime (INCC) e o Plano Tático de Combate a Crimes Cibernéticos, desenvolvidos pelo Ministério da Justiça e Segurança Pública, são exemplos de esforços concretos para fortalecer a segurança digital no país. Essas ações estão alinhadas com as diretrizes estabelecidas pelo Decreto Lei n.º 10.222/2020, que sancionou a Estratégia Nacional de Segurança Cibernética (E-Ciber), demonstrando um compromisso com a proteção de infraestruturas críticas e a privacidade dos cidadãos.

Por sua vez, o Decreto Lei n.º 11.856/2023 representa um avanço significativo na política de segurança cibernética nacional. Com a criação da Política Nacional de Cibersegurança (PNCiber) e do Comitê Nacional de Cibersegurança (CNCiber), o decreto visa desenvolver tecnologias nacionais, garantir a integridade dos dados e aumentar a resiliência contra ameaças cibernéticas. Essas medidas refletem a importância crescente da cibersegurança no cenário atual, onde a informação é um ativo valioso e a segurança digital é fundamental para a soberania de uma nação.

É importante ressaltar que os resultados obtidos nesta pesquisa têm impacto não apenas na área de estudo, mas também em toda a sociedade. A proteção dos dados pessoais dos cidadãos brasileiros e a promoção da segurança digital são questões de interesse público, que requerem ações coordenadas e efetivas por parte das autoridades e profissionais envolvidos.

Portanto, esta pesquisa contribui para o entendimento das nuances e desafios dos crimes cibernéticos, reforçando a importância da legislação, da perícia digital e do investimento em capacitação profissional. À medida que avançamos na era digital, é fundamental estar preparado para enfrentar as ameaças emergentes e garantir um ambiente online seguro e confiável para todos os usuários.

6. REFERÊNCIAS

1. ARAUJO, Karolaine Rayala Balsanulfo; COUTO, Stephani Reis Oliveira. Investigação e Atualização: Abordando a Complexidade dos Crimes Cibernéticos na Sociedade Moderna. Trabalho de Conclusão de Curso (Bacharel em Direito). Goianésia: Faculdade Evangélica de Goianésia, 2023.
2. BISPO, Adrielle da Silva; BINTO, Emanuel Vieira. Crimes Cibernéticos: Da Ineficácia Da Lei Carolina Dieckmann Na Prática De Crimes Virtuais. Revista Ibero-Americana de Humanidades, Ciências e Educação, [S. l.], v. 9, n. 11, p. 354–369, 2023. DOI: 10.51891/rease.v9i11.12291. Disponível em: https://periodicorease.pro.br. Acesso em: 17 mar. 2024.
3. BRASIL. Código Penal Brasileiro. Decreto Lei nº 2.848 de 07 de dezembro de 1940. Disponível em:http://www.planalto.gov.br. Acesso em: 20 fev. 2024.
4. BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988.
5. BRASIL. Decreto-Lei n.º 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética.. Diário

Oficial da União, Brasília, DF, 6 fev. 2020. Disponível em: https://www.planalto.gov.br. Acesso em: 25 mar. 2024.
6. BRASIL. Decreto-Lei n.º 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança.. Diário Oficial da União, Brasília, DF. Disponível em: https://www.planalto.gov.br. Acesso em: 20 fev. 2024.
7. BRASIL. Instituto Nacional De Combate ao Cibercrime. Disponível em: https://incc.org.br. Acesso em: 08 abr. 2024.
8. BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br. Acesso em: 10 fev. 2024.
9. BRASIL. Lei n.º 14.155, de 27 de maio de 2021. Dispõe sobre crimes cometidos por meio da internet ou por sistema eletrônico, informático ou telemático, e dá outras providências. Diário Oficial da União, Brasília, DF, 27 mai. 2021. Disponível em: https://www.planalto.gov.br. Acesso em: 20 fev. 2024.
10. BRASIL. Lei n° 12.737, de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br. Acesso em: 10 fev. 2024.
11. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br. Acesso em: 09 fev. 2024.
12. BRASIL. Marco Civil da Internet. Lei nº 12.965 de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br. Acesso em: 25 fev. 2024.
13. BRASIL. Sistema de Pagamentos Brasileiro. Banco Central do Brasil, 2021. Disponível em https://www.bcb.gov.br. Acesso em 10 mar. 2024
14. CARMO, Marcus Fábio Fontenelle do. Introdução sobre a perícia digital, apresentando conceitos e metodologia. Curitiba, Paraná (PR), 2020. Disponível em: https://academiadeforensedigital.com.br. Acesso em: 19 mar. 2024.
15. DATAREPORTAL. Digital Brazil 2024. Disponível em: https://datareportal.com. Acesso em: Acesso em: 10 mar. 2024.
16. DUARTE, Samuel Victor. Crimes Cibernéticos. 2022. Trabalho de Conclusão de Curso (TCC) - Faculdade Cidade de João Pinheiro – FCJP, João Pinheiro.
17. FORTINET. Brasil é o segundo país que mais sofre ataques cibernéticos na América Latina. Disponível em: https://www.fortinet.com. Acesso em: 03 mar. 2024.
18. FORTINET. Threat Predictions: Chained AI and CAAS Operations. Disponível em:https://www.fortinet.com. Acesso em: 03 mar. 2024.
19. FRANCK, K. M., & FERREIRA, R. V. Instruções preventivas contra crimes cybernéticos e orientações da perícia forense computacional. Revista Nativa Americana de Ciências, Tecnologia & Inovação, v. 4, n. 1, 116-132, 2023. Disponível em: https://jiparana.emnuvens.com.br. Acesso em 10 mar. 2024.
20. gação relacionadas aos crimes cibernéticos de estelionato na rede social WhatsApp. Revista Científica UNIFAGOC - Jurídica, v. 7, n. 2, 2022
21. KASPERSKY LAB. Panorama de Ciberameaças 2023. Disponível em: https://www.kaspersky.com.br/blog/panorama-de-ciberameacas-2023/21631/. Acesso em 10 mar. 2024
22. LAKATOS, Eva M. Fundamentos de Metodologia Científica. São Paulo: Grupo GEN, 2021. E-book. ISBN 9788597026580. Disponível em: https://integrada.minhabiblioteca.com.br. Acesso em: 11 abr. 2024.
23. LIMA, Milena Angela Santos. Cibercrimes: A Vulnerabilidade dos Usuários. 2022. Trabalho de Curso (Bacharelado em Direito) - Escola de Direito e Relações Internacionais, Pontifícia Universidade Católica de Goiás, Goiânia, 2022.
24. LORENZO, Larissa Papandreus; SCARAVELLI, Gabriela Piva. Cibercrimes e a legislação brasileira. Diálogos e interfaces do Direito – Revista Científica do Curso de Direito, Centro Universitário FAG, 2020.
25. MAIA, Teymisso Sebastian Fernandes. Análise dos Mecanismos de Combate aos Crimes Cibernéticos no Sistema Penal Brasileiro. Monografia (Graduação em Direito) - Universidade Federal do Ceará, Faculdade de Direito, Fortaleza, 2017.
26. MARTINS, Humberto. Seminário virtual: Criminalidade em tempo de Covid. Atuação do Sistema de Justiça. Disponível em: https://www.stj.jus.br. Acesso em: 19 mar. 2024.
27. MASSON, Cleber. Direito Penal - Parte Especial (arts. 121 a 212) - Vol. 2.São Pualo: Grupo GEN, 2024. E-book. ISBN 9786559649525. Disponível em: https://integrada.minhabiblioteca.com.br/

. Acesso em: 15 mar. 2024.
28. Ministério da Justiça e Segurança Pública (MJSP). Plano Tático de Combate a Crimes Cibernéticos. 22 de março de 2022. Disponível em: https://www.gov.br. Acesso em: 17 mar. 2024.
29. MIRANDA, Lucas Eller Freitas de Alencar. Os Impactos da Falta de Punição para o Crime de Estelionato Digital no Brasil. 2023. Trabalho de Conclusão de Curso (Bacharel em Direito) - Universidade Federal de Juiz de Fora, Campus Governador Valadares.
30. OLIVEIRA, Daiana Souza de; SANTIAGO, Vinícius Vale; COSTA, Adriana Vieira da. Perícia Forense Computacional: A Admissibilidade e a Fragilidade Das Evidências Coletadas via Computação Forense. Revista Ibero-Americana de Humanidades, Ciências e Educação, [S. l.], v. 9, n. 5, p. 3978–3997, 2023. DOI: 10.51891/rease.v9i5.10087. Disponível em: https://periodicorease.pro.br. Acesso em: 17 mar. 2024.
31. PEDROSA, João Marcelo Braga Fernandes; COLTRO, Rafael Khalil. A problemática da adequação típica nos crimes eletrônicos: uma análise prática da conduta nos crimes cometidos através do sistema PIX. In: FULLER, Greice Patrícia (Coord.). Crimes, dignidade da pessoa humana e Sociedade da Informação: Direito Penal Digital e Arte. Centro Universitário das Faculdades Metropolitanas Unidas, 2022. Disponível em: https://mestradodireito.fmu.br Acesso em: Acesso em 10 mar. 2024
32. PINHEIRO, Patrícia P. Direito Digital. São Paulo: Editora Saraiva, 2021. E-book. ISBN 9786555598438. Disponível em: https://integrada.minhabiblioteca.com.br. Acesso em: 27 fev. 2024.
33. POLÍCIA CIVIL DO DISTRITO FEDERAL. Polícia alerta para alta nos golpes envolvendo o Pix. Disponível em: https://www.pcdf.df.gov.br. Acesso em: 20 mar. 2024 .
34. SANTOS, Bianca Stefany Ribeiro dos. Crimes cibernéticos no Brasil: invasão de dispositivo informático e estelionato virtual. Goiânia: Pontifícia Universidade Católica de Goiás, 2023.
35. SILVA FILHO, WILSON . Anatomia do Modus Operandi de um Cracker - Perícia de um Caso Real de Fraudes pela Internet. In: The Tenth International Conference on Forensic Computer Science and Cyber Law, 2018. Proceedings of The Tenth International Conference on Forensic Computer Science and Cyber Law.
36. SILVA, Eva Cristina de Souza. Proteção contra os crimes cibernéticos no Brasil: a necessidade de uma legislação específica e atualizada. Artigo Científico (Trabalho de Curso II). Pontifícia Universidade Católica de Goiás - Escola de Direito e Relações Internacionais, 2021
37. SILVA, Milene Meneze. Crimes Cibernéticos: Uma Análise da Lei Carolina Dieckmann. São Paulo: Universidade São Judas Tadeu, 2023. Trabalho de Conclusão de Curso (Bacharel em Direito) – Universidade São Judas Tadeu, São Paulo, 2023.
38. SILVA, Moacir Antunes; CARVALHO, Urssula Rodrigues. Análise sobre as dificuldades de investi
39. TEIXEIRA, Tarcisio. Direito Digital e Processo Eletrônico. São Paulo: Editora Saraiva, 2022. E-book. ISBN 9786555596946. Disponível em: https://integrada.minhabiblioteca.com.br. Acesso em: 15 mar. 2024.
40. WORLD ECONOMIC FORUM. Global Cybersecurity Outlook 2024. 2024. Disponível em: https://www3.weforum.org/Acesso em : 27 fev. 2024.
41. ZAMBONATO, Matheus Schultz. Avanços da legislação brasileira no combate aos crimes cibernéticos. Trabalho de Conclusão de Curso, Porto Alegre, RS. 2022. Disponível em: http://hdl.handle.net. Acesso em 10 mar. 2024