REVISTA OWL (*OWL Journal*)
www.revistaowl.com.br – ISSN: 2965-2634

OS CRIMES CIBERNÉTICOS E AS FRAUDES DE DADOS NAS REDES SOCIAIS

CYBERCRIMES AND DATA FRAUD ON SOCIAL MEDIA

DOI: 10.5281/zenodo.15446633

Luciano da Cruz Santos [1]
Thiago Borges Andrade[2]

RESUMO

O presente trabalho visa compreender os crimes cibernéticos e as fraudes de dados nas redes sociais que emergem como fenômenos complexos e preocupantes na era digital. Com a crescente utilização dessas plataformas, usuários se tornam alvos vulneráveis para diversas práticas fraudulentas, como roubo de identidade, *phishing* e disseminação de informações falsas. A facilidade de acesso e compartilhamento de dados pessoais favorece a atuação de criminosos digitais, que exploram brechas na segurança das redes. Estudos indicam que as fraudes em redes sociais não só comprometem a privacidade dos indivíduos, mas também afetam a integridade de empresas e organizações. As implicações econômicas são significativas, uma vez que a confiança no ambiente virtual é prejudicada. Além disso, a legislação sobre crimes cibernéticos ainda está em desenvolvimento em muitos países, o que dificulta a responsabilização efetiva dos infratores. Portanto, a conscientização sobre segurança digital e a implementação de políticas mais rigorosas são essenciais para mitigar os riscos associados às fraudes de dados, promovendo um ambiente online mais seguro e confiável para todos os usuários.

Palavras-Chave: Crimes Cibernéticos. Internet. Fraudes nas Redes Sociais.

1 Acadêmico do 10 período do Curso de Direito do Centro Universitário UniBRAS Rio Verde.
2 Professor Mestre do Curso de Direito do Instituto de Centro Universitário UniBRAS Rio Verde e orientador da pesquisa.

REVISTA OWL (*OWL Journal*)
www.revistaowl.com.br – ISSN: 2965-2634

ABSTRACT

This paper aims to understand cybercrimes and data fraud on social networks, which are emerging as complex and worrying phenomena in the digital age. With the increasing use of these platforms, users become vulnerable targets for various fraudulent practices, such as identity theft, phishing and the dissemination of false information. The ease of accessing and sharing personal data favors the actions of digital criminals, who exploit gaps in network security. Studies indicate that fraud on social networks not only compromises the privacy of individuals, but also affects the integrity of companies and organizations. The economic implications are significant, since trust in the virtual environment is undermined. In addition, cybercrime legislation is still under development in many countries, which makes it difficult to effectively hold offenders accountable. Therefore, awareness of digital security and the implementation of stricter policies are essential to mitigate the risks associated with data fraud, promoting a safer and more reliable online environment for all users.

Keywords: Cybercrimes. Internet. Social Media Scams.

INTRODUÇÃO

A expansão da Internet tem sido notável nas últimas décadas, refletindo um aumento contínuo no número de usuários globalmente. Dentre os fatores que impulsionam essa tendência, destaca-se a evolução tecnológica, que tem proporcionado conexões mais rápidas e estáveis, além de inovações significativas em dispositivos de acesso.

A acessibilidade também desempenha um papel crucial: a popularização de computadores e dispositivos móveis, como smartphones e tablets, democratizou o uso da Internet, permitindo que uma diversidade maior de indivíduos interaja com o meio digital. Dessa forma, a combinação desses elementos contribui para a inclusão digital e a ampliação do alcance da Internet na sociedade contemporânea (Araújo, 2023).

Os crimes cibernéticos e as fraudes de dados nas redes sociais têm se tornado um problema crescente na era digital. Esses delitos envolvem o uso da tecnologia para realizar atividades ilícitas, como roubo de identidade, vazamento de informações pessoais e fraudes financeiras. As redes sociais, por sua natureza interativa, tornam-se alvos atraentes para os criminosos, que exploram a vulnerabilidade dos usuários para coletar dados sensíveis e programar esquemas fraudulentos.

Um dos principais fatores que contribuem para a proliferação desses crimes é a falta de conscientização dos usuários sobre práticas seguras de navegação e privacidade. Além disso, a facilidade de acesso às plataformas digitais e a escassez de regulamentações rigorosas facilitam a ação dos infratores. Medidas de segurança, como autenticação em dois fatores e campanhas de educação em cibersegurança, são essenciais para mitigar esses riscos e proteger os dados dos usuários.

As autoridades e plataformas de redes sociais também desempenham um papel crucial na luta contra esses crimes. A implementação de políticas mais rígidas para a proteção de dados e a colaboração entre órgãos de segurança pública e empresas de tecnologia são estratégias necessárias para coibir a atuação dos criminosos. Portanto, a conscientização e a colaboração entre todos os envolvidos são fundamentais para enfrentar os desafios impostos pelos crimes cibernéticos.

No entanto, a legislação brasileira sobre crimes cibernéticos está em constante evolução para acompanhar as mudanças tecnológicas e as novas modalidades de crimes que surgem nesse ambiente. As leis existentes, como a Lei Carolina Dieckmann, o Marco Civil da Internet e a LGPD, representam importantes esforços nesse sentido, estabelecendo um marco regulatório robusto e abrangente para a proteção dos direitos dos usuários e a punição dos infratores no ambiente digital.

A problemática deste estudo é averiguar como a norma penal brasileira já regulamentada no ordenamento jurídico é efetiva em virtude dos crimes praticados virtualmente? Quais os parâmetros utilizados para a elucidação dos casos de crimes cibernéticos no Brasil? Partindo da hipótese de que é possível acontecer os crimes cibernéticos em razão da não proteção de dados dos usuários de redes sociais. E visa reconhecer os crimes cibernéticos e ter uma maior compreensão dos crimes praticados, partindo de uma análise geral para demonstrar como são praticados estes crimes que acontecem diariamente no espaço virtual.

No atual momento, em que a discussão no mundo se dá acerca da necessidade de proteção de dados para diminuição dos crimes realizados através das plataformas virtuais,

visando combater esses crimes, por se tratar de grandes números de ataques acontecidos diariamente, que vem ocasionando grandes prejuízos para população do ciberespaço, que tem seus dados violados e expostos.

A pesquisa tem como objetivo geral analisar a importância da preservação dos dados das redes mundiais de computadores e telefonia, sendo de grande importância a proteção dos dados neles informados, para o não acontecimento de crimes praticados através da invasão de dados.

Crimes cibernéticos têm se tornado uma preocupação crescente em todo o mundo, especialmente com a popularização das redes sociais. Este trabalho aborda as diferentes formas como esses crimes se manifestam nas plataformas digitais, bem como as fraudes de dados que ocorrem nesse ambiente. Serão discutidas as consequências sociais e legais, além de estratégias de prevenção e mitigação.

O avanço da tecnologia e a ascensão das redes sociais transformaram a forma como indivíduos e empresas interagem. Contudo, essa evolução trouxe consigo uma gama de riscos, sendo os crimes cibernéticos e as fraudes de dados alguns dos mais preocupantes. As redes sociais, ao facilitarem o compartilhamento de informações, tornam-se um alvo propício para atividades ilícitas.

1. METODOLOGIA

Este estudo será realizado através de uma revisão bibliográfica de caráter descritivo e abordagem qualitativa. Conforme Marconi e Lakatos (2006), a pesquisa bibliográfica abrange publicações em relação ao tema de estudo, como: publicações avulsas, boletins, jornais, revistas, livros, pesquisas, monografias, teses, material cartográfico, rádio, gravações em fita magnética, filmes e até televisão, onde sua finalidade é colocar o pesquisador em contato direto com o que foi escrito, dito ou filmado sobre determinado assunto.

De acordo com Gil (2024, p. 73),

> A revisão da literatura promove o levantamento acerca do que já se conhece em relação ao assunto que está sendo pesquisado. Possibilita, portanto, identificar lacunas no conhecimento existente e, consequentemente, orientar a pesquisa com o propósito de preenchê-las.

Segundo Gil (2024), esse levantamento sistemático é fundamental para identificar lacunas que ainda não foram exploradas na literatura acadêmica. Ao reconhecer essas lacunas, o pesquisador pode direcionar sua investigação de forma mais assertiva, buscando responder a perguntas que ainda permanecem sem resposta e, assim, contribuir para o avanço do conhecimento na área de estudo.

A revisão da literatura é um componente essencial no processo de pesquisa, pois não apenas compila e analisa o conhecimento já existente sobre um determinado tema, mas também estabelece um contexto que permite compreender a evolução das ideias e teorias relacionadas.

A coleta de dados será realizada por meio de busca online das produções científicas sobre, compreendendo o período de 2015 a 2023, com exceção de artigos de relevância, para levantamento de bibliografia, com publicações em língua portuguesa, artigos científicos, periódicos do CAPES, dissertações e livros; através do sistema on-line, entre outros e da Biblioteca Central da Universidade, pertinentes ao tema.

Desse modo, a revisão da literatura atua como um guia metodológico, auxiliando na escolha de abordagens e técnicas que são mais adequadas para a pesquisa em questão. Ela permite ao pesquisador estruturar suas hipóteses de forma fundamentada, apoiando-se em evidências teóricas e empíricas já estabelecidas. Essa articulação entre o que já se conhece e o que se pretende investigar torna a pesquisa mais robusta e legitimada, favorecendo a construção de um conhecimento mais profundo e significativo. Portanto, a revisão da literatura não pode ser vista apenas como uma formalidade, mas sim como um passo crucial para garantir a relevância e a eficácia de qualquer pesquisa científica.

Segundo Gil (2024, 175),

> A análise qualitativa não difere da análise quantitativa unicamente porque envolve descrições verbais e não números. As diferenças têm a ver com a

> própria natureza das duas modalidades de investigação. A pesquisa quantitativa tem como fundamentos os pressupostos da abordagem positivista, que admitem a existência de uma única realidade objetiva. Já a pesquisa qualitativa, embora decorrente de múltiplas tradições, baseia-se no pressuposto de que a realidade pode ser vista sob múltiplas perspectivas.

A análise qualitativa e a análise quantitativa são frequentemente distinguidas por suas metodologias e resultados, mas essa diferença vai além da simples escolha entre descrições verbais ou dados numéricos. Segundo Gil (2024), enquanto a pesquisa quantitativa se fundamenta em pressupostos positivistas que consideram uma única realidade objetiva, a pesquisa qualitativa abraça uma visão mais pluralista e interpretativa.

Essa abordagem reconhece que a realidade é complexa e multifacetada, permitindo assim que múltiplas perspectivas sejam exploradas e compreendidas. Assim, a pesquisa qualitativa não se limita a mensurar fenômenos, mas busca entender os significados e contextos associados a eles, promovendo um entendimento mais profundo das experiências humanas.

Portanto, a natureza da coleta de dados e da análise nas duas abordagens reflete essas diferenças fundamentais. Na pesquisa quantitativa, a ênfase está na objetividade e na generalização dos resultados, utilizando instrumentos padronizados e técnicas estatísticas para validar hipóteses. Em contraste, a pesquisa qualitativa utiliza métodos como: entrevistas, grupos focais e observações, que permitem uma aproximação mais rica e contextualizada com o objeto de estudo.

2. REVISÃO DA LITERATURA

2.1. INTERNET

A internet é uma vastíssima rede capaz de interligar computadores de todo o mundo, possibilitando, assim, a comunicação entre eles. Ela surgiu na década de 60, mais precisamente no ano de 1966, quando algumas universidades se uniram para desenvolver a ARPANET (Advanced Research Projects Administration – Administração de Projetos e Pesquisas Avançados). Naquela oportunidade, seu uso era exclusivo das Forças Armadas

norte-americanas. Seu propósito era prover um contínuo funcionamento daquela rede, mesmo em casos de calamidade como um ataque nuclear. Destarte, era de suma importância não haver um comando central que pudesse ser alvejado. Este é o típico retrato do medo causado pela Guerra Fria, que dominava o mundo naquela época (Crespo, 2011).

A internet, conforme destacado por Wendt (2023), transformou-se em uma ferramenta multifacetada que abrange diversas áreas da vida contemporânea. Desde a facilitação de conversas comerciais e networking até o acesso a um vasto universo de conhecimento, suas aplicações são quase ilimitadas. As pessoas usam a internet não apenas para se conectar e manter relacionamentos, mas também para desenvolver atividades de marketing pessoal e entretenimento. Essa versatilidade contribui para um crescimento exponencial do uso da tecnologia, refletindo como a rede global se tornou intrínseca à rotina diária de milhões.

No entanto, essa ascensão da internet também traz consigo desafios significativos. À medida que mais pessoas se conectam, o potencial para o uso indevido da plataforma aumenta. Wendt (2023) ressalta que, em alguns casos, a interação online pode resultar em transtornos para terceiros, incluindo perdas financeiras consideráveis para as vítimas. Este cenário destaca a importância da conscientização sobre segurança digital e da necessidade de estratégias eficazes para mitigar esses riscos, garantindo que a internet continue sendo um ambiente positivo e produtivo para todos os usuários.

É inerente a esta sociedade que o acesso livre às tecnologias e à rede seja um direito de todos os cidadãos. Mais do que isso, garantias e liberdades constitucionais passam a ser consideradas e refletidas à luz dos impactos que as novas tecnologias trazem no dia a dia. Nas escolas, no trabalho ou nas relações pessoais, estar online é realidade, não no mero contexto de estar conectado, mas no sentido de estar incluído digitalmente, algo além do tradicional ler e escrever, diga-se, ser um ser social digital, estar “em rede”. Para muitos, vivemos em uma sociedade absolutamente discriminatória. Entre os riscos, a substituição da escola, onde jovens amoldados a novas tecnologias poderiam entender que elas, “por si sós”, podem lhes proporcionar todo o conhecimento necessário para viver (Jesus, 2016).

Jesus (2016) entende que por debaixo do capô desta sociedade, uma infraestrutura de meios comunicativos que interliga os continentes. Na sociedade da informação, muitas vezes passa despercebido o aparato estrutural destinado a suportar as comunicações e, por que não dizer, suportar as relações sociais, que se passam no mundo dos bits. Vivemos uma sociedade em que nos comunicamos muito, sem saber como tal comunicação é possível, como, quando e por onde. A dominância informacional é flagrante, embora nem todos reconheçam. E informação é poder.

No Brasil adotou-se primeiramente a legislação criminal (que deveria ser a última *ratio*), de modo a punir condutas praticadas por intermédio ou contra sistemas informáticos. Os direitos dos usuários vieram depois com a Lei n. 12.965/2014, denominada "Marco Civil da Internet". Uma sociedade que não está preparada para entender o que pode caracterizar ou não um crime informático, mas que a despeito já o tipifica, inconsequentemente (Jesus, 2016).

Para Jesus (2016), foi apenas posteriormente, que os direitos dos usuários de internet ganharam destaque, com a promulgação da Lei n. 12.965/2014, conhecida como "Marco Civil da Internet". Essa lei não apenas estabeleceu diretrizes para o uso da internet no Brasil, mas também buscou garantir a proteção e a privacidade dos usuários em um cenário digital em constante evolução. Contudo, a implementação efetiva dessa legislação enfrenta desafios significativos. As faltas de entendimento sobre os aspectos da criminalidade digital e a insuficiência de educação e informação acerca dos direitos e deveres dos usuários acabam por criar um ambiente propício à confusão e à insegurança. Assim, é essencial promover um diálogo mais profundo sobre a intersecção entre tecnologia, direito e sociedade, para que possamos avançar em direção a um futuro digital mais justo e equitativo.

2.2. MARCO CIVIL DA INTERNET

O Marco Civil da Internet, instituído pela Lei nº 12.965 em 23 de abril de 2014, representa um marco fundamental na regulação do uso da internet no Brasil, estabelecendo princípios, direitos e deveres que visam garantir a proteção dos usuários e a promoção de uma rede mais justa e acessível. A legislação busca preencher uma lacuna importante ao introduzir

normas claras para o ciberespaço, abordando questões como a privacidade dos dados, a neutralidade da rede e a responsabilidade dos provedores de serviços. Com isso, o Marco Civil não apenas reforça a importância da internet como um espaço democrático, mas também assegura que todos os cidadãos tenham acesso a um ambiente virtual seguro e respeitoso, promovendo a cidadania digital (Barreto, 2016).

O dispositivo em questão consolidou a aplicação da legislação brasileira, especificamente a Lei Geral de Proteção de Dados (LGPD), ao estabelecer que sua incidência abrange todas as etapas do ciclo de tratamento de dados pessoais quando qualquer delas ocorre em território nacional. Isso significa que, independentemente de onde esteja localizado o controlador ou processador dos dados, se a coleta, armazenamento ou uso ocorrer no Brasil, às normas e diretrizes da LGPD se aplicam.

Essa medida é fundamental para proteger os direitos dos titulares dos dados, garantindo que suas informações sejam tratadas de maneira ética e transparente, promovendo a segurança jurídica e a confiança nas relações digitais. Como destaca Lima (2020), essa definição robusta do alcance da legislação reforça a importância da proteção de dados em um mundo cada vez mais conectado.

O Marco Civil da Internet dispõe, em seu art. 11, regras sobre o âmbito de aplicação espacial da lei quanto a proteção dos dados pessoais e a privacidade.

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil. § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil. § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da

> legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações. § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo. (Brasil, 2014)

O Art. 11 do Marco Civil da Internet (2014) estabelece diretrizes essenciais para a coleta, armazenamento e tratamento de dados pessoais e de comunicações realizadas por provedores, enfatizando a importância de respeitar a privacidade dos usuários. A norma é clara ao afirmar que todas as operações devem ocorrer em conformidade com as leis brasileiras, especialmente quando se refere a registros e dados que, mesmo que tratados por entidades estrangeiras, atinjam cidadãos brasileiros ou sejam realizados no território nacional. Essa abordagem protege não apenas os direitos individuais dos brasileiros, mas também assegura um padrão elevado de responsabilidade para as empresas que operam neste âmbito.

Além disso, de acordo com o Marco Civil da Internet (2014), em seu parágrafo 1º reafirma que qualquer dado coletado em solo brasileiro deve obedecer às mesmas regras, independentemente da localização geográfica do provedor. O art. 2º estende essa obrigação a empresas internacionais que oferecem serviços ao público brasileiro, promovendo uma proteção abrangente aos dados mesmo fora das fronteiras. Por fim, os parágrafos subsequentes destacam a necessidade de transparência na operação dessas plataformas, exigindo que forneçam informações que comprovem o cumprimento da legislação, assim como estabelecendo mecanismos regulatórios para investigar possíveis infrações. Desta maneira, a legislação cria um ambiente mais seguro e confiável, tanto para usuários quanto para provedores de serviços digitais no Brasil.

Desse modo salienta-se que, haja a neutralidade da rede, proibindo a discriminação de dados, a proteção de dados pessoais, onde se regulamenta a coleta, uso, armazenamento e tratamento de dados pessoais na internet, bem como promover a responsabilidade dos provedores, a fim de definir as responsabilidades civis de provedores de serviços de internet.

2.3. CRIMES CIBERNÉTICOS

Os crimes cibernéticos são crimes realizados através dos computadores, celulares e outros quaisquer meios de telecomunicação digitais. Que é definido como ato humano caracterizado por fatos típicos, conduta ilegal e negligência na utilização dos dispositivos que vem facilitando as execuções de crimes causando danos a qualquer pessoa que se utiliza os meios virtuais.

Os crimes digitais têm ganhado uma relevância crescente na sociedade contemporânea, especialmente em um mundo cada vez mais interconectado e dependente da tecnologia. Entre as condutas que se destacam, o acesso não autorizado a sistemas informáticos revela-se um dos principais problemas enfrentados por organizações e indivíduos. Esse tipo de infração não apenas compromete a integridade e a confidencialidade de dados sensíveis, mas também pode resultar em consequências financeiras e reputacionais severas. Ademais, ações destrutivas dentro desses sistemas, que podem incluir a instalação de *malware* ou ataques de *ransomware*, trazem à tona a necessidade de reavaliar as medidas de segurança cibernética e a legislação pertinente, buscando uma resposta adequada a essa nova realidade digital.

Para Crespo (2011), além das questões já mencionadas, a interceptação de comunicações e as modificações de dados figuram como preocupações prementes no contexto dos crimes digitais. Essas práticas violam não apenas a privacidade individual, mas também os direitos fundamentais de comunicação entre cidadãos. Outros crimes, como infrações a direitos autorais, incitação ao ódio, discriminação, escárnio religioso e a difusão de pornografia infantil, demonstram a diversidade e a gravidade das ofensas que podem ser perpetradas no ambiente virtual.

O terrorismo cibernético, por sua vez, coloca em xeque a segurança nacional e global, exigindo a adoção de estratégias multifacetadas para sua prevenção e combate. Assim, a análise sistemática dessas condutas ilícitas é fundamental para a elaboração de políticas públicas eficazes, bem como para a conscientização da sociedade sobre a importância da ética digital.

Ainda de acordo com Crespo (2011), o ciberespaço se configura como um ambiente complexo e multifacetado que, embora não esteja isento de regulamentações jurídicas tradicionais, apresenta desafios únicos na tipificação de delitos. Muitas condutas que antes eram restritas ao espaço físico, agora ganham nova dimensão no virtual, tornando-se suscetíveis a variadas interpretações legais. O avanço tecnológico supera, em muitas ocasiões, a capacidade do legislador de acompanhar e regular as novas práticas ilícitas que emergem nesse espaço. Assim, fenômenos como o *cyberbullying*, fraudes eletrônicas e vazamentos de dados pessoais, por exemplo, demandam uma atenção especial da legislação para que possam ser adequadamente tratadas dentro do arcabouço jurídico brasileiro.

Além dos delitos já tipificados, o ciberespaço abriga práticas nocivas que, até o momento, não possuem uma tipificação clara nas leis brasileiras. A vulnerabilidade intrínseca desse ambiente permite que ações prejudiciais, como a disseminação de desinformação e discursos de ódio, proliferem sem a devida responsabilização legal. Isso impõe um desafio crítico tanto para a sociedade quanto para os órgãos responsáveis pela elaboração e aplicação das leis. Portanto, é crucial que o debate sobre a regulação do ciberespaço avance, promovendo um equilíbrio entre a proteção dos direitos individuais e a liberdade de expressão, enquanto se busca uma abordagem proativa para a prevenção e punição de condutas ilícitas nessa nova fronteira digital (Crespo, 2011).

A proteção de dados e dispositivos informáticos emerge como um dos pilares fundamentais na sociedade contemporânea, caracterizada pela intensa digitalização das interações sociais. Segundo Bitencourt (2023), tal proteção não se limita apenas aos aspectos técnicos da segurança cibernética, mas abrange a salvaguarda dos conteúdos que são armazenados e processados, considerando-os elementos essenciais da privacidade individual. Essa preocupação com a privacidade, tanto em esferas pessoais quanto profissionais, se configura como um princípio de ordem pública que deve ser amplamente respeitado e defendido. O respeito a esse princípio não apenas se alinha às necessidades individuais de proteção, mas também reflete um compromisso mais amplo com a dignidade e o respeito à

autonomia dos indivíduos em um cenário onde as informações pessoais são cada vez mais vulneráveis a abusos e acessos não autorizados.

Ademais, a proteção penal, conforme indicado por Bitencourt (2023), deve ser vista como um mecanismo que visa garantir a inviolabilidade da privacidade, o que implica em uma resposta adequada a qualquer violação desse direito. Em vez de focar exclusivamente na infraestrutura da rede mundial de computadores, a abordagem deve priorizar a proteção do indivíduo ofendido, assegurando que seus dados e informações privadas não sejam comprometidos. Esse enfoque não apenas reforça a confiança dos cidadãos nas tecnologias digitais, mas também promove um ambiente mais seguro e ético para a troca de informações. Assim, a implementação e o fortalecimento de legislações voltadas à proteção de dados pessoais tornam-se imperativos, refletindo uma evolução necessária nas normas sociais e jurídicas que regem a vida em um mundo digitalizado.

Gonçalves (2020) destaca que a promulgação da Lei n. 12.737/2012 representou um marco significativo na abordagem legislativa dos crimes cibernéticos no Brasil, uma vez que, antes de sua aprovação, a responsabilização penal por delitos desta natureza ocorria exclusivamente sob a ótica da legislação comum. Nesse contexto, a tipificação de crimes cibernéticos era inadequada e limitava a efetividade das punições, pois eram exigidos resultados concretos, como a subtração de valores ou danos materiais e morais à vítima, para que qualquer medida punitiva fosse possível. A nova legislação trouxe uma série de dispositivos específicos que visam coibir práticas ilícitas no ambiente digital, permitindo uma resposta mais ágil e eficaz por parte do sistema judicial frente aos desafios impostos pela evolução da tecnologia e pela crescente incidência de delitos virtuais.

A fim de antecipar a possibilidade de punição dos criminosos virtuais que disseminam vírus ou arquivos espiões pela rede ou invadem dispositivos informáticos alheios, para aplicação de golpes, a referida lei também conhecida como Lei Carolina Dieckman, introduziu em seu art. 154-A o disposto:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou

> informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput (Brasil, 2012).

A Lei Carolina Dieckman, sancionada em 2012, representa um importante avanço na legislação brasileira no que diz respeito à proteção dos dispositivos informáticos e à segurança cibernética. O artigo 154-A, que estabelece a penalização para a invasão de dispositivos alheios, reflete uma preocupação crescente com os crimes virtuais e as suas implicações sociais e econômicas. Ao tipificar como crime a ação de invadir dispositivos, roubar dados ou instalar programas maliciosos sem a autorização do usuário, a lei busca criar um ambiente digital mais seguro, protegendo tanto os indivíduos quanto as organizações contra práticas ilícitas que podem causar danos irreparáveis (Brasil, 2012).

Além disso, a norma se estende à responsabilização daqueles que produzem, oferecem ou disseminam software com a intenção de facilitar tais invasões. Essa extensão da responsabilidade penal é uma medida necessária para coibir não apenas a prática direta de crimes cibernéticos, mas também o mercado paralelo que sustenta e propaga essas atividades ilícitas. Com penas que vão de três meses a um ano de detenção, acompanhadas de multas, a Lei Carolina Dieckman busca não apenas punir, mas também desestimular a prática de crimes na internet, promovendo uma cultura de maior respeito à privacidade e à integridade dos dados dos usuários. A efetividade da aplicação dessa legislação, no entanto, depende da conscientização dos cidadãos sobre a importância da segurança digital e da atuação eficaz das autoridades competentes na fiscalização e repressão a esses delitos (Brasil, 2012).

Conforme destacado por Gonçalves (2020), a análise do tipo penal revela que a violação de um computador pode ocorrer independentemente da sua conexão à internet. Embora a prática comum envolva a exploração de sistemas online, torna-se evidente que é viável a instalação de programas maliciosos em máquinas desconectadas, permitindo a captura de dados sensíveis, como imagens e mensagens.

Esses programas, muitas vezes instalados de maneira presencial, possibilitam ao agente infrator a coleta clandestina de informações, as quais são posteriormente transferidas fisicamente para fora do sistema comprometido. Esta abordagem, embora menos frequente, demonstra a versatilidade das técnicas de invasão e a necessidade de uma compreensão abrangente dos riscos associados à segurança cibernética.

3. CONCLUSÃO

A expansão da Internet nas últimas décadas tem sido realmente impressionante, evidenciada pelo crescimento exponencial no número de usuários ao redor do mundo. Esta tendência é fortemente impulsionada por avanços tecnológicos que não apenas melhoraram a infraestrutura de conectividade, mas também democratizaram o acesso à rede global.

A introdução de tecnologias como a fibra óptica e redes móveis de alta velocidade tem permitido que mais pessoas se conectem com rapidez e confiabilidade, enquanto inovações em dispositivos, como smartphones e tablets, têm facilitado o acesso à Internet em uma variedade de contextos.

Os crimes cibernéticos e as fraudes de dados nas redes sociais emergem como fenômenos complexos que demandam uma análise aprofundada, especialmente em um contexto em que o uso dessas plataformas se torna cada vez mais comum e indispensável na vida cotidiana dos indivíduos. A vulnerabilidade dos usuários é ampliada pela facilidade com que informações pessoais são compartilhadas, criando um terreno fértil para práticas fraudulentas, como roubo de identidade e *phishing*.

O uso indevido de dados pessoais não apenas compromete a privacidade individual, mas também altera a dinâmica das relações entre consumidores e empresas, impactando negativamente na confiança que os usuários depositam no ambiente digital. As pesquisas indicam que a disseminação de informações falsas nas redes sociais pode gerar desestabilização social e econômica, pois os consumidores, inseguros sobre a veracidade das informações, tornam-se hesitantes em suas decisões de compra e interação.

Além das implicações individuais e empresariais, a lacuna legislativa em muitos países em relação aos crimes cibernéticos representa um desafio significativo para a proteção dos dados e a responsabilização dos infratores. A adoção de políticas mais rigorosas e práticas de segurança são essenciais para criar um ambiente online mais seguro, onde a confiança possa ser restaurada e mantida.

Portanto, é imperativo que governos, organizações e usuários colaborem para enfrentar esses desafios, promovendo uma cultura de segurança cibernética que beneficie toda a sociedade.

REFERÊNCIAS

ARAÚJO, Cláudio Rodrigues. Crimes Virtuais. Belo Horizonte - Editora Expert - 2023

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. Manual de investigação cibernética: à luz do marco civil da internet. 1. Ed. Rio de Janeiro: Brasport, 2016.

BITENCOURT, Cezar R. Tratado de direito penal: parte especial. Crimes contra a pessoa (ARTS. 121 A 154-B). V.2. São Paulo: SRV Editora Ltda., 2023. E-BOOK. ISBN 9786553627031. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553627031/. Acesso em: 05 jun. 2024.

BRASIL. [Código Penal (1940)] Código penal. Brasília, DF: Presidência da República. 1940.

BRASIL. Lei nº 12.737 de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos, 2013.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Marco Civil da Internet).

CRESPO, Marcelo Xavier de F. Crimes digitais. São Paulo: SRV Editora Ltda., 2011. E-book. ISBN 9788502136663. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502136663/. Acesso em: 05 jun. 2024.

GONÇALVES, Victor Eduardo R. Sinopses jurídicas v 08 - direito penal: dos crimes contra a pessoa. São Paulo: SRV Editora Ltda., 2020. E-book. ISBN 9786555592337. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555592337/. Acesso em: 05 jun. 2024.

JESUS, Damásio de; MILAGRE, José a. Manual de crimes informáticos. São Paulo: SRV Editora Ltda, 2016. E-book. ISBN 9788502627246. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502627246/. Acesso em: 05 jun. 2024.

LIMA, Cíntia Rosa Pereira de. Comentários à lei geral de proteção de dados. São Paulo: Grupo Almedina, 2020. E-book. ISBN 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 05 jun. 2024.

WENDT, Emerson. Crimes Cibernéticos. 2ª edição – Ameaças e procedimentos de investigação / Emerson Wendt; Higor Vinicius Nogueira Jorge. – 2. Ed. – Rio de Janeiro: Brasport, 2013.

https://www.jusbrasil.com.br/topicos/28004011/artigo-154a-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940

Recebido em: 04/04/2025
Aprovado em: 15/04/2025
Publicado em: 16/05/2025