Código de defesa do consumidor e Lei Geral de Proteção de Dados: Vulnerabilidade e aplicabilidade acerca dos golpes digitais

Lindemberg Passos Neto [1], Carlos Henrique Passos Mairink[2]

Resumo: Este estudo aborda os desafios dos crimes informáticos e as ferramentas de prevenção e repressão na era digital. Contextualiza a crescente vulnerabilidade dos consumidores na internet e analisa leis como a Lei Carolina Dieckmann e a LGPD. O objetivo geral desta monografia é investigar a conexão digital e os desafios dos crimes informáticos, destacando a evolução legislativa nacional e internacional e as diversas tipologias de crimes cibernéticos. Utilizando uma metodologia bibliográfica qualitativa, os principais resultados destacam avanços legislativos e tecnológicos, mas ressaltam a necessidade de atualização contínua e cooperação internacional. A transformação digital, acelerada pelo uso massivo da internet e dispositivos conectados, tem proporcionado inúmeros benefícios econômicos, sociais e culturais. No entanto, essa mesma transformação expõe indivíduos, empresas e governos a novos e complexos tipos de crimes, que desafiam os métodos tradicionais de prevenção e repressão. Os resultados mostraram que os crimes informáticos, que vão desde fraudes e roubos de identidade até ataques cibernéticos sofisticados contra infraestruturas críticas, representam uma ameaça significativa à segurança, à privacidade e à confiança dos usuários na era digital. Esses delitos não só causam danos financeiros e materiais, mas também podem comprometer a integridade e a estabilidade das instituições e processos democráticos. Neste contexto, o Direito Penal desempenha um papel essencial na definição, tipificação e punição desses crimes, buscando proteger os direitos dos cidadãos e garantir a ordem social. A análise das ferramentas legais e tecnológicas de prevenção e repressão aos crimes informáticos é, portanto, de extrema importância para identificar as lacunas existentes na legislação e na prática, bem como para propor melhorias e adaptações necessárias. Além disso, a constante evolução das tecnologias exige uma atualização contínua das medidas de segurança e das estratégias de combate aos crimes cibernéticos. A cooperação internacional emerge como um fator crucial, visto que a natureza global da internet facilita a atuação de criminosos além das fronteiras nacionais. A harmonização das legislações e a colaboração entre países são essenciais para uma resposta efetiva a essas ameaças. Conclui-se que uma abordagem integrada, envolvendo educação digital e medidas preventivas e repressivas, é essencial para a segurança cibernética e a proteção dos usuários.

[1] Aluno do Curso de Direito da Famig. Faculdade Minas Gerais.

[2] Revisor. Professor do Curso de Direito da Famig. Faculdade Minas Gerais

Palavras-chave: crimes informáticos; direito penal; prevenção; repressão; era digital.

Consumer protection code and General Data Protection Law: Vulnerability and applicability regarding digital fraud

Abstract: This study addresses the challenges of computer crimes and prevention and repression tools in the digital age. It contextualizes the growing vulnerability of consumers on the internet and analyzes laws such as the Carolina Dieckmann Law and the LGPD. The general objective of this monograph is to investigate the digital connection and the challenges of computer crimes, highlighting national and international legislative developments and the different types of cyber crimes. Using a qualitative bibliographic methodology, the main results highlight legislative and technological advances, but highlight the need for continuous updating and international cooperation. Digital transformation, accelerated by the massive use of the internet and connected devices, has provided numerous economic, social and cultural benefits. However, this same transformation exposes individuals, companies and governments to new and complex types of crimes, which challenge traditional methods of prevention and repression. The results showed that cybercrimes, ranging from fraud and identity theft to sophisticated cyberattacks against critical infrastructure, pose a significant threat to users' security, privacy and trust in the digital age. These crimes not only cause financial and material damage, but can also compromise the integrity and stability of democratic institutions and processes. In this context, Criminal Law plays an essential role in defining, classifying and punishing these crimes, seeking to protect citizens' rights and guarantee social order. The analysis of legal and technological tools for preventing and repressing computer crimes is, therefore, extremely important to identify existing gaps in legislation and practice, as well as to propose necessary improvements and adaptations. Furthermore, the constant evolution of technologies requires a continuous update of security measures and strategies to combat cybercrime. International cooperation emerges as a crucial factor, given that the global nature of the internet facilitates the actions of criminals beyond national borders. Harmonization of legislation and collaboration between countries are essential for an effective response to these threats. It is concluded that an integrated approach, involving digital education and preventive and repressive measures, is essential for cybersecurity and user protection.

Keywords: computer crimes; criminal law; prevention; repression; digital age.

1 INTRODUÇÃO

No contexto atual, a transformação digital e a evolução das tecnologias da informação têm revolucionado diversos aspectos da vida cotidiana e das relações comerciais. Com a popularização da internet e o crescente uso de dispositivos

conectados, surgem novas oportunidades, mas também novos desafios, especialmente no que diz respeito à segurança e à integridade das interações online (MOURA, 2021).

Este cenário tem gerado um aumento significativo dos crimes informáticos, que se tornam cada vez mais sofisticados e difíceis de combater. A presente monografia se propõe a explorar esses fenômenos, analisando a vulnerabilidade acentuada pela internet e as medidas legislativas e tecnológicas adotadas para enfrentar esses desafios (LIMA, 2021).

O objetivo geral desta monografia é investigar a conexão digital e os desafios dos crimes informáticos, destacando a evolução legislativa nacional e internacional e as diversas tipologias de crimes cibernéticos. Especificamente, busca-se analisar como a internet acentua a vulnerabilidade dos consumidores nas relações comerciais, estudar a tipologia e a classificação dos crimes informáticos, e examinar as ferramentas de prevenção e repressão a esses crimes. Para tanto, serão considerados diferentes tipos de crimes informáticos, como golpes nas relações de consumo, pedofilia online, crimes contra a honra, cyberbullying e estelionato, além de legislações específicas como a Lei Carolina Dieckmann e a Lei nº 13.709 de 14 de agosto de 2018.

A justificativa para esta pesquisa reside na necessidade urgente de compreender e mitigar os impactos dos crimes informáticos na sociedade contemporânea. Com o aumento exponencial do uso da internet para fins comerciais, educacionais e pessoais, os usuários estão cada vez mais expostos a diversas formas de ataques cibernéticos. A análise das vulnerabilidades e a efetividade das medidas legislativas e tecnológicas são fundamentais para a proteção dos consumidores e para a manutenção da confiança no ambiente digital.

A metodologia adotada nesta monografia será predominantemente bibliográfica e qualitativa, utilizando-se de livros, artigos acadêmicos disponíveis no Google Acadêmico e na plataforma SICELO, entre outros. A pesquisa qualitativa permitirá uma análise aprofundada dos conceitos e das implicações dos crimes informáticos a revisão bibliográfica fornecerá uma base teórica sólida para a

discussão dos temas abordados. A coleta de dados será realizada através de fontes secundárias, priorizando estudos recentes e relevantes que contribuam para a compreensão do fenômeno em análise.

O problema de pesquisa que norteia este estudo é: "Como a evolução tecnológica e a expansão da internet têm acentuado a vulnerabilidade dos consumidores e quais são as medidas legislativas e tecnológicas mais eficazes para a prevenção e repressão dos crimes informáticos?" Através dessa questão, pretende-se identificar as principais falhas e desafios no combate aos crimes cibernéticos, bem como propor soluções e estratégias que possam ser adotadas para aumentar a segurança e a proteção dos usuários no ambiente digital.

2 CONEXÃO DIGITAL E OS DESAFIOS DOS CRIMES INFORMÁTICOS

Na atualidade, a internet se transformou em um espaço onde os usuários compartilham informações sobre suas vidas, por meio de redes sociais, transações bancárias via aplicativos, downloads, envio de e-mails, cadastros em sites e outros diversos cliques ao longo de suas navegações. No entanto, após a realização desses procedimentos na rede, o usuário perde o controle sobre o destino e a propagação das informações fornecidas. Esses conteúdos podem ser alterados ou interpretados de maneiras diversas, tornando-se crucial a intervenção do Estado para reprimir os ilícitos e prevenir a sociedade dos perigos presentes no universo cibernético (SILVA, 2017).

Segundo Garcia (2016), diversos termos têm sido empregados na literatura para descrever o comportamento delituoso relacionado a computadores, tais como: ciber criminalidade (computer-related crime), crime cibernético (cybercrime), crime tecnológico (technological crime), crime assistido por computador (computer-assisted crime), crimes digitais (digital crime), crimes eletrônicos (electronic crime) e crime da Internet (Internet crime).

Conforme Almeida et al. (2015), a cibernética é definida como a ciência que estuda os sistemas informantes, especialmente os sistemas de informação. Com base no conceito analítico de crime, as referidas autoras concluem que os "crimes cibernéticos" são todas as ações que se enquadram nos critérios de tipicidade,

ilicitude e culpabilidade e que são praticadas contra ou com o uso dos sistemas de informática.

Jesus e Milagres (2016) compreendem que os crimes virtuais se caracterizam como condutas típicas e ilícitas praticadas por meio da tecnologia da informação, ou ainda, contra ela, ou seja, um ato ilícito cometido por meio de informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Para Garcia (2016), um traço comum entre essas definições é a utilização indevida de dispositivos tecnológicos por indivíduos, grupos ou organizações que detêm conhecimentos avançados na área de Tecnologia da Informação.

A dinâmica da sociedade contemporânea é moldada pela constante evolução tecnológica, que tem como propósito facilitar e encurtar as relações humanas. A busca incessante pela melhor versão de si mesmo leva os indivíduos a recorrerem ao meio digital como um facilitador dessas interações. Nesse contexto, a Internet surge como uma ferramenta essencial na conexão entre computadores, originando novas formas de interação tanto no âmbito pessoal quanto profissional (Moura, 2021).

No contexto pessoal, as pessoas buscam estabelecer relações mais profundas, transcendendo a barreira da tela e transformando interações virtuais em experiências reais. No campo profissional, a tecnologia proporciona uma gama de possibilidades, desde a flexibilidade de horários até a viabilização do trabalho remoto, permitindo uma conciliação entre vida pessoal e profissional.

É inegável que a tecnologia se tornou indispensável para a vida em sociedade. Entretanto, as rápidas mudanças trazidas pelo progresso tecnológico também apresentam desafios. As vantagens incluem a facilitação das relações amorosas, de consumo e jurídicas. Enquanto facilita diversas áreas da vida, a tecnologia também traz consigo riscos e desvantagens. A velocidade das informações e das interações torna cada vez mais complexo definir limites para seu uso, e o crescimento do acesso indiscriminado à internet facilita a prática de crimes, muitas vezes sem punição adequada.

Assim como no mundo físico, na internet também existem indivíduos propensos a práticas ilícitas. O anonimato proporcionado pelo ambiente virtual é um dos principais fatores que contribuem para o aumento do nível de crimes. Estes crimes podem acarretar consequências devastadoras para as vítimas, já que a violação da privacidade online pode afetar não apenas aspectos pessoais, mas também profissionais e todos os aspectos de suas vidas.

Exemplos desses crimes incluem a divulgação de dados bancários para golpes financeiros, vazamento de conversas íntimas nas redes sociais, o que pode levar a danos significativos e o aumento preocupante nos casos de pedofilia, especialmente pela falta de supervisão de adultos sobre o uso da Internet por crianças. A confiança nas interações online torna-se uma tarefa desafiadora, pois a verdadeira identidade e intenções por trás das telas são muitas vezes difíceis de discernir.

Assim, enquanto o mundo digital oferece inúmeras vantagens, também abre as portas para um novo tipo de criminalidade, deixando a sociedade vulnerável e suscetível. Crimes como esses que muitas vezes não conseguem ser solucionados, nem ao menos se pode identificar o autor, faz com que gere na sociedade certa sensação de impunidade.

A divulgação de informações pessoais e sigilosas na rede pode nos tornar vulneráveis a uma nova forma de criminalidade, exigindo uma abordagem cautelosa e consciente ao utilizar a tecnologia (Moura, 2021).

Horbylon (2022) amplia o conceito de crimes virtuais, destacando que eles podem envolver uma pluralidade de sujeitos. Por exemplo, um hacker que é contratado para roubar informações corporativas de um concorrente pode usar seu conhecimento em explorar falhas de segurança em um sistema. Nesse caso, além do contratante, do hacker e da vítima (concorrente), outros sujeitos podem estar envolvidos.

2.1 DA TECNOLOGIA

A tecnologia é um meio fundamental para entender os crimes informáticos, uma vez que, é através dela que indivíduos utilizam a Internet para cometerem tais crimes. Diante da possibilidade do anonimato, permite que os criminosos ajam contra qualquer pessoa conectada a uma rede. A internet é um meio facilitador para prática de atos ilícitos e divulgação de informações (Moura, 2021).

Por exemplo, o roubo de dados pessoais, fraudes bancárias e ataques cibernéticos. De acordo com o dicionário Michaelis, a tecnologia é definida por:

> Conjunto de processos, métodos, técnicas e ferramentas relativos à arte, indústria, educação, etc.; Conhecimento técnico e científico e suas aplicações a um campo particular; tudo o que é novo em matéria de conhecimento técnico e científico; linguagem peculiar a um ramo determinado do conhecimento, teórico ou prático; aplicação dos conhecimentos científicos à produção em geral.

O surgimento de novos métodos de aplicação dessa tecnologia, estão cada vez mais presente no cotidiano humano, que definem alterações diversas nas relações sociais e econômicas (Moura, 2021).

A Internet apresenta desafios únicos para a aplicação da lei e a investigação de crimes informáticos (Crespo, 2011). Os criminosos podem operar de qualquer lugar do mundo, dificultando a identificação e responsabilização. Além disso, as fronteiras digitais não são delimitadas, o que na maioria das vezes dificulta na aplicação da lei. Para conceituar Internet Ticiane Morais Franco (2014, p. 19) ressalta:

> A internet como um sistema de rede aberta, expressa na liberdade do fluxo de informação, a partir de uma rede internacional de computadores conectados entre si, que possibilita o intercâmbio de informações e a transferência de arquivos de toda a natureza, entre máquinas que estejam conectadas a uma rede, por meio do protocolo de rede TCR-IP (Transmission Control Protocol/Internet Protocol).

Para combater os crimes informáticos de forma eficaz, é necessário um entendimento claro do ambiente da Internet e das tecnologias envolvidas. Isso inclui a implementação de medidas de segurança cibernética robustas, a cooperação entre governos e empresas, e o fortalecimento das capacidades de investigação e aplicação

da lei no âmbito digital. A compreensão do papel da Internet nos crimes informáticos é essencial para desenvolver estratégias eficazes de prevenção e combate a essa forma de criminalidade em constante evolução (Bioni, 2018).

No que se refere à natureza jurídica dos crimes cibernéticos, Orrigo e Figueira (2015) mencionam a existência de diversas classificações doutrinárias. Os crimes cibernéticos próprios, por exemplo, são aqueles em que o uso do computador é essencial para a sua prática, ou seja, o agente precisa do computador para cometer o delito, e os bens jurídicos afetados pelos crimes cibernéticos próprios são os dados que estão armazenados em outros sistemas ou redes.

Já uma outra categoria, conhecida como crimes virtuais impróprio, é conceituada por Lima (2021) como condutas típicas, antijurídicas e culpáveis que são cometidas por meio de ferramentas informáticas, mas que poderiam ter sido praticadas por outros meios. Coelho e Branco (2016) aprofundam esse conceito, destacando que dentro dessa categoria encontram-se crimes comuns do cotidiano, como é o caso do discurso de ódio na internet, que tem desafiado o equilíbrio entre o direito constitucional à liberdade de expressão e a proteção de direitos fundamentais, como a honra, a imagem, a privacidade e a intimidade. É fundamental ponderar esses direitos em cada caso concreto.

Entretanto, segundo Marra (2019), há ainda três outras categorias de crimes cibernéticos, que são o crime informático puro, o crime de informática misto e o crime informático comum. O crime informático puro diz respeito ao dano causado diretamente ao sistema de informática, em que o agente busca corromper os dados do computador da vítima, através de vírus e outros meios similares.

O crime de informática misto, por sua vez, ocorre quando a violação do bem jurídico lesado não está diretamente ligada ao sistema de informática, mas este é um instrumento necessário para a prática do delito, como acontece no caso de furto eletrônico de contas bancárias. Por fim, o crime informático comum é aquele que já está previsto na lei penal, podendo ou não ser cometido através do uso do computador, como é o caso de crimes como pedofilia, racismo e cyberbullying (Gomes, 2021).

A fraude cibernética representa uma ameaça significativa para as fintechs, podendo resultar em prejuízos financeiros e danos à reputação das instituições. Diversos tipos de fraudes cibernéticas são perpetrados, como phishing, malware, roubo de identidade e ataques a sistemas de pagamento. Essas práticas criminosas envolvem o uso indevido de informações pessoais e financeiras dos usuários, comprometendo a segurança das transações e dos dados (Dhamija et al., 2007).

2.1.1 Método de phishing

O método de *phishing* é amplamente documentado na literatura acadêmica e em relatórios de segurança cibernética e é definido como:

> Uma forma de ataque cibernético que envolve o uso de técnicas enganosas, como e-mails ou sites fraudulentos, para induzir os usuários a revelar informações confidenciais, como credenciais de login ou dados financeiros. Esses ataques exploram táticas de engenharia social e falhas de design em interfaces de usuário, tornando difícil até mesmo para usuários cautelosos detectar e evitar serem vítimas de tais golpes (Dhamija et al., 2006).

O *phishing* é uma técnica de fraude cibernética em que os fraudadores se passam por entidades confiáveis, como instituições financeiras, empresas ou órgãos governamentais, para enganar as vítimas e obter informações sensíveis, como senhas, números de cartão de crédito ou dados pessoais (Ribeiro,2022). Os golpes de *phishing* geralmente ocorrem por meio de e-mails, mensagens de texto ou até mesmo por telefonemas, nos quais os fraudadores tentam convencer as pessoas a compartilharem suas informações confidenciais. Essas mensagens costumam ser convincentes e podem conter links maliciosos que direcionam as vítimas a sites falsos, onde os dados são capturados.

Uma vez que os fraudadores obtêm essas informações, eles podem usá-las para acessar contas bancárias, realizar transações fraudulentas, roubar identidades ou cometer outros tipos de crimes financeiros (Ribeiro,2022).

Para se proteger do *phishing*, é importante adotar algumas medidas de segurança. Isso inclui a verificação cuidadosa dos remetentes de e-mails e mensagens, evitando clicar em links suspeitos ou fornecer informações pessoais sem verificar a autenticidade da solicitação. Além disso, é fundamental manter os

dispositivos atualizados com softwares de segurança e antivírus, além de utilizar senhas fortes e únicas para cada conta (DHAMIJA et al., 2006). As empresas e instituições financeiras também desempenham um papel importante na prevenção do *phishing*, implementando medidas de segurança, como filtros de spam, autenticação em duas etapas e programas de conscientização e treinamento para seus funcionários e clientes.

Para Szor (2005), a fraude cibernética em fintechs é um desafio crítico que precisa ser abordado. Com o rápido crescimento das fintechs e o aumento das transações financeiras online, os fraudadores têm encontrado oportunidades para explorar vulnerabilidades e realizar atividades fraudulentas.

2.1.2 Malware

A prática de *Malware* (software malicioso) é uma das principais ameaças enfrentadas na segurança cibernética. Consiste na criação e disseminação de programas maliciosos que visam infectar sistemas, dispositivos ou redes com o objetivo de causar danos, obter informações sensíveis ou controlar remotamente os recursos comprometidos. Segundo Christodorescu (2008, p.69):

> A detecção de *malware* envolve o desenvolvimento de técnicas e ferramentas para identificar e mitigar a presença de software malicioso em sistemas de computador. É uma tarefa desafiadora devido à crescente complexidade e sofisticação do malware, exigindo análises avançadas e mecanismos de detecção para ficar à frente das ameaças em evolução.

Os malwares podem assumir diferentes formas, como vírus, *worms*, cavalos de Troia, *ransomware* e *spyware*, entre outros. Eles são distribuídos através de métodos como anexos de e-mail, downloads de arquivos infectados, links maliciosos e exploração de vulnerabilidades em sistemas e aplicativos desatualizados. Uma vez que o malware é executado no dispositivo ou sistema-alvo, ele pode roubar informações, comprometer a integridade dos dados, interromper serviços, realizar atividades fraudulentas ou fornecer acesso não autorizado a recursos.

> *Malware* refere-se a software malicioso projetado para se infiltrar em sistemas de computador, comprometer sua integridade e executar ações não autorizadas. Abrange uma ampla variedade de programas maliciosos, como vírus, *worms*, cavalos de Tróia e

> *spyware*, que representam ameaças significativas à segurança de redes de computadores e privacidade dos usuários (Szor,2005, p.26).

Os danos causados pelo malware podem ser extensos, incluindo a perda de dados importantes, interrupção de serviços essenciais, prejuízos financeiros, danos à reputação da empresa e violação da privacidade dos usuários. Além disso, os ataques de malware são frequentemente utilizados como vetor de entrada para outros tipos de ataques, como o roubo de identidade, fraude financeira e espionagem cibernética.

2.1.3 Vulnerabilidade Acentuada Pela Internet

Diante da atual sociedade de consumo em massa, agravada pelo crescente uso da internet como meio de propagação das estratégias de marketing publicitário, seria inadequado afirmar que a manifestação de vontade do consumidor é plenamente livre. A oferta de produtos e serviços por meios virtuais exerce um poder persuasivo considerável, muitas vezes de maneira inconsciente. Apesar de o direito teórico assegurar a liberdade e autonomia dos contratantes, na prática, é evidente o desequilíbrio resultante dessas relações (Silva; Martins; Marques Filho, 2022).

Nesse contexto, torna-se notório o desequilíbrio existente entre o consumidor e o fornecedor, o que impulsionou a necessidade de uma proteção diferenciada por parte do Estado, em consonância com o princípio da igualdade, visando alcançar um mínimo de equilíbrio nas relações de consumo. Nessa perspectiva, o Código de Defesa do Consumidor, em seu artigo 4º, inciso I, estabelece que a vulnerabilidade do consumidor no mercado de consumo deve ser considerada como um dos objetivos do referido código (BRASIL, 1990).

A condição de fragilidade experimentada pelo consumidor individual deve ser compreendida como um dos princípios fundamentais do Código. De acordo com a abordagem de Almeida e Lenza (2020), tal princípio reconhece a existência de disparidades na relação de consumo, enfatiza a posição do consumidor como parte mais vulnerável do contrato e garante uma abordagem diferenciada por meio de instrumentos legais capazes de restabelecer o equilíbrio entre fornecedor e consumidor. É importante ressaltar que a vulnerabilidade mencionada nos artigos

supracitados não deve ser confundida com a hiper vulnerabilidade, que se refere a um grupo específico de consumidores com características pessoais que os tornam ainda mais suscetíveis às relações de consumo. Conforme descrito:

> "[...] a vulnerabilidade inerente à relação de consumo é combinada com uma vulnerabilidade intrínseca à pessoa do consumidor, seja devido à sua idade (crianças e idosos), condição de saúde (doentes), necessidades especiais (pessoas com deficiência) ou nível de escolaridade (analfabetos), tornando-os mais propensos a ceder às pressões exercidas pelos fornecedores. Assim, a hiper vulnerabilidade surge como resultado da sobreposição dessas características pessoais que fragilizam o indivíduo - verificáveis no caso concreto - à vulnerabilidade relacional do consumidor, resultando em um consumidor-criança, consumidor-idoso, consumidor-doente, consumidor-deficiente ou consumidor-analfabeto que requer atenção especial por parte do Estado. Essa atenção deve ser exercida por meio de suas instituições legislativas, órgãos públicos responsáveis pelo controle e fiscalização das atividades econômicas no mercado de consumo e pelos magistrados encarregados de decidir casos envolvendo esses atores, sempre considerando essas hiper vulnerabilidades como uma diretriz para sua atuação" (Canto, 2014, p. 76-77).

O artigo XXXII do inciso 5º da Constituição da República Federativa do Brasil de 1988 estabelece que o Estado possui o dever de promover a defesa do consumidor como um direito e garantia fundamental. Além disso, o texto constitucional, ao tratar das disposições legais sobre a ordem econômica, enfatiza a importância do princípio da defesa do consumidor, indicando que a ordem econômica deve ser pautada nesse princípio (art. 170, inciso V da CRFB/88). Dessa forma, a proteção dos consumidores é considerada um dos fundamentos da ordem econômica no Brasil (BRASIL, 1988).

Essas disposições legais demonstram a relevância atribuída pelo legislador brasileiro às relações de consumo, especialmente devido à disparidade existente entre as partes envolvidas. De acordo com as considerações de Bruno Miragem, os direitos do consumidor justificam-se pela constatação de sua vulnerabilidade, a qual é presumida de forma absoluta e constitui uma característica intrínseca desse ramo do direito (Thiago, 2022).

Segundo o autor mencionado, a noção de vulnerabilidade no direito das relações de consumo está relacionada à identificação de fraqueza ou debilidade de

um dos sujeitos da relação jurídica (consumidor), em decorrência de determinadas condições ou características intrínsecas, bem como à existência de uma posição de força que pode ser observada no outro sujeito da relação jurídica. É importante ressaltar que esse princípio está vinculado ao princípio da isonomia, uma vez que busca tratar de forma diferenciada aqueles que se encontram em situações desiguais, visando alcançar a igualdade desejada.

Na maioria das relações estabelecidas no mercado de consumo, constata-se que o consumidor ocupa uma posição de maior vulnerabilidade. Diante disso, torna-se indispensável proporcionar-lhe um tratamento diferenciado, visando alcançar uma igualdade substancial em relação ao fornecedor. A proteção e a busca pela igualdade nas relações de consumo são preceitos consagrados na Constituição Federal, que, inclusive, resultaram na criação do Código de Defesa do Consumidor (Aliceral, 2014).

A assimetria de informações é caracterizada pela disparidade de conhecimento entre os diferentes agentes econômicos envolvidos em uma transação. Nesse contexto, ocorre uma situação em que os consumidores, que possuem um nível de informação limitado, realizam negociações com vendedores que detêm um conhecimento mais abrangente. Tal disparidade resulta em problemas relacionados à seleção adversa e ao risco moral (Rodrigues; Daldi, 2017).

No contexto digital, observa-se uma manifestação singular do desequilíbrio nas interações comerciais, relacionadas ao consumo, adquirindo atributos distintos que merecem ser minuciosamente analisados pela literatura especializada e pela jurisprudência. É indubitável que, quando tais interações ocorrem na plataforma global conhecida como World Wide Web, a expertise e proficiência técnica e tecnológica conferem ao fornecedor uma vantagem adicional em relação ao consumidor, fator capaz de acentuar a disparidade entre as partes envolvidas (Modenesi, 2010).

No ambiente virtual, frequentemente ocorre uma situação que acentua a condição de vulnerabilidade do consumidor como parte mais frágil na relação de consumo. A ausência de contato presencial entre as partes torna o consumidor mais

propenso a falta de informações, aumentando o risco de suas dúvidas serem esclarecidas pelo fornecedor.

Embora o Código de Defesa do Consumidor estabeleça a obrigação legal do fornecedor de fornecer informações claras e adequadas sobre os produtos e serviços oferecidos, tais informações muitas vezes são apresentadas de maneira insuficiente ou obscurecida, dificultando o diálogo direto do consumidor com o fornecedor no contexto do comércio eletrônico. Como resultado, se as informações essenciais sobre os produtos frequentemente não são divulgadas nos anúncios, muito menos é mencionada a finalidade para a qual os dados pessoais fornecidos pelo consumidor no momento da celebração do contrato de compra são destinados. Além disso, apenas uma pequena parcela dos consumidores possui conhecimento sobre o valor dos seus dados pessoais e a necessidade de protegê-los adequadamente (Cardoso, 2022).

Em situações de assimetria informacional, é comum a ocorrência de conflitos de interesse decorrentes dessa disparidade de conhecimento. Nesse contexto, podem ser identificados dois problemas decorrentes da assimetria informacional: o problema de seleção adversa, que se manifesta quando uma das partes do mercado não possui a capacidade de observar o tipo ou a qualidade dos bens e serviços oferecidos pela outra parte; e o problema de risco moral, que ocorre quando uma das partes do mercado não consegue monitorar as ações da outra parte (Fonseca, 2022).

Considerando a existência de assimetrias informacionais nos mercados, as quais acarretam efeitos desestabilizadores e contribuem para ineficiências e desequilíbrios, é necessário reconhecer a importância de superar essa assimetria por parte dos agentes econômicos. No contexto das relações de consumo, as adversidades decorrentes das assimetrias informacionais tendem a agravar ainda mais a relação naturalmente desequilibrada, evidenciando assim a necessidade de instituições capazes de mitigar os efeitos indesejados das informações imperfeitas inerentes a tais relações (Nascimento, 2015).

De fato, a assimetria informacional nos contratos de consumo representa uma falha que amplifica o desequilíbrio entre fornecedores e consumidores de produtos e serviços. É evidente que, na ausência de informações adequadas que permitam ao consumidor avaliar a qualidade ou o preço dos produtos, ocorre um desequilíbrio no mercado. Nessa situação, os consumidores podem se tornar reféns dos fornecedores de produtos e serviços de má qualidade, bem como dos preços por eles praticados (Czelusniak, 2019).

Por essa razão, torna-se imperativo que haja intervenção estatal por meio de normas consumeristas que protejam o direito à informação, buscando reduzir ou, ao menos, mitigar a assimetria informacional entre consumidores e fornecedores. Tal intervenção visa proteger não apenas a dignidade humana dos consumidores vulneráveis, mas também o próprio mercado consumerista, evitando comportamentos prejudiciais e estimulando o consumo (Nascimento, 2015).

2.2 A evolução legislativa nacional e internacional contra a repressão dos crimes informáticos

A legislação passa por transformações para se adequar às diversas mudanças no Brasil, bem como em outros países ao redor do mundo. Essa evolução legislativa tem sido impulsionada pela necessidade de lidar com os desafios enfrentados pelo Direito diante do avanço tecnológico, visando garantir a segurança no meio informático (Bioni, 2018).

Um marco importante na legislação brasileira contra crimes informáticos foi a promulgação da lei que disciplina o uso da Internet no Brasil, a Lei nº 12.965/14, também conhecido como Marco Civil da Internet, que institui:

> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
>
> - o reconhecimento da escala mundial da rede;
>
> - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
>
> - a pluralidade e a diversidade; IV - a abertura e a colaboração;
>
> - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

- a finalidade social da rede.

Assim como demais pautas de discussão, diversos autores, como Luiz Flávio Gomes, Grégore Moreira de Moura, abordam questões relacionadas a cerca da segurança na internet. Gomes, por exemplo, discorre sobre o avanço tecnológico e a necessidade da legislação acompanhar as diversas atualizações.

No âmbito internacional, diversos tratados e convenções têm sido estabelecidos para promover a cooperação entre os países na repressão aos crimes informáticos. O Brasil é signatário de tratados como a Convenção de Budapeste, também conhecida como a Convenção sobre o Crime cibernético, firmada em Budapeste, em 23 de novembro de 2001, que estabelece medidas para prevenir e combater crimes informáticos.

A Convenção de Budapeste, em seu Preâmbulo, diz que:

> Convencidos de que a presente Convenção é necessária para impedir ações conduzidas contra a confidencialidade, a integridade e a disponibilidade de sistemas informáticos, redes e dados de computador, bem como para impedir o abuso de tais sistemas, redes e dados, ao prever a criminalização de tais condutas, tal como se encontram descritas nesta Convenção, e ao prever a criação de competências suficientes para combater efetivamente tais crimes, facilitando a descoberta, a investigação e o julgamento dessas infrações penais em instâncias domésticas e internacionais, e ao estabelecer mecanismos para uma cooperação internacional rápida e confiável; Atentos para a necessidade de assegurar o devido equilíbrio entre os interesses dos órgãos de persecução criminal e o respeito aos direitos humanos fundamentais, tal como previstos na Convenção Europeia para a Proteção dos Direitos Humanos e Liberdades Fundamentais, de 1950, no Pacto das Nações Unidas sobre Direitos Civis e Políticos, de 1966, bem como em outros tratados internacionais sobre direitos humanos que reafirmem o direito universal à liberdade de consciência, sem interferência de qualquer espécie, bem como o direito à liberdade de expressão, que inclui a liberdade de buscar, receber e compartilhar informações e ideias de qualquer espécie, independentemente de limites, e os direitos à intimidade e à privacidade.

Em suma, reforça a necessidade de uma cooperação internacional, em prol de uma evolução legislativa, visto que os avanços na tecnologia e as novas formas de crimes informáticos exigem adaptações constantes das leis. A cooperação internacional com a criação de convenções, tratados e a cooperação internacional é

meio fundamental para a prevenção e combates de tais crimes, promovendo a integrada e segurança na era digital.

Segundo Moura (2021, p 56) a adesão do Brasil à Convenção de Budapeste, consagra a universalidade do combate aos crimes informáticos, além de buscar maior efetividade e união de esforços entres os países signatários, ainda que não esteja dentro do eixo do Conselho Europeu, o que é bom, visto que o problema não é local e sim mundial.

2.3 Análise sobre a tipologia e classificação dos crimes informáticos

As denominações que fazem referência aos crimes praticados no mundo digital são inúmeras, não há um consenso sobre qual denominação usada para se referir a esses delitos, crimes de computação, delitos de informática, fraude informática, assim os conceitos ainda não englobam todos os crimes ligados à tecnologia (Crespo, 2011, p. 48).

A ciência que tem como objeto de estudo as informações automatizadas (dados) é a Informática. Esta é a ciência que estuda os meios para armazenar, processar e transmitir dados, ou seja, para registrar, manipular e transmitir informações de forma automatizada. A própria origem da palavra informática 'derivou da junção dos vocábulos informação e automática, cuja criação é atribuída ao francês Philippe Dreyfus, embora, também, impute-se a autoria da expressão a Karkevitch e a Dorman' (Pimentel, 2000, p.29). Assim, está claro que a denominação mais precisa para os delitos ora em estudo é 'crimes informáticos' ou 'delitos informáticos', por se basear no bem jurídico penalmente tutelado que é a inviolabilidade das informações automatizadas (dados).

No crime informático, é fundamental considerar não apenas a definição geral de crime, mas também o contexto em que o crime ocorre. Diferentemente dos crimes convencionais, os crimes informáticos não se desenrolam diretamente entre o agressor e a vítima, mas sim através de uma interface digital, onde o contato físico é inexistente. Como vítima e agressor estão geograficamente distantes, essa distinção é fundamental para a observância de interações que ocorrem nesse âmbito virtual (BIONI, 2018).

Quanto à classificação dos tecnocrimes, também há diversos entendimentos doutrinários que podem levar em consideração os bens jurídicos violados, os procedimentos adotados para cometimento da infração ou o objetivo final da conduta praticada (Ferreira, 2000).

A classificação mais aceita pelos estudiosos do Direito, conforme proposta pela autora mencionada acima, se baseia na forma de execução dos crimes, dividindo-os em próprios, praticados diretamente por meio de dispositivos informáticos com o intuito de prejudicar os bens jurídicos oriundos das relações digitais, e impróprios, nos quais a ferramenta digital é utilizada apenas como meio para atingir qualquer bem jurídico protegido (Ferreira, 2000).

Os crimes informáticos podem ser classificados como crimes informáticos próprios, impróprios, crimes informáticos mistos e crimes informáticos mediatos ou indiretos. Também conhecidos como cibercrimes, os crimes informáticos próprios são aqueles em que o objetivo é atingir a informação, nesse o agente explora as vulnerabilidades dos sistemas computacionais, ficando evidente que o bem jurídico lesado pela inviolabilidade da informação automatizada. Por exemplo, podemos citar o crime de invasão de dispositivo, a inserção de dados falsos em sistemas de informação e a modificação ou alteração não autorizada de sistema de informações, ambos dispostos respectivamente nos artigos 154-A, 313-A E 313-B do Código Penal Brasileiro (Bioni, 2018).

Já nos crimes informáticos impróprios o que caracteriza tal modalidade é que são facilitados ou aprimorados pelo uso de computadores ou tecnologia digital, os exemplos mais comuns são os crimes contra o patrimônio, honra, entre outros, onde computador se torna mero instrumento do agente e objetivo final é a vontade do infrator.

Os crimes mistos são aqueles que envolvem tanto elementos digitais quanto físicos, esses crimes combinam a tecnologia ao mundo físico, por exemplo, a transferência bancária de forma ilícita, nesse caso existe mais de um bem jurídico tutelado.

Por fim, nos crimes mediatos ou indiretos são aqueles em que a tecnologia é utilizada como meio ou um facilitar para cometer outros tipos de crime, podendo incluir fraude, extorsão, dentre outros.

Em suma, a classificação dos crimes informáticos é importante para reconhecer a complexidade e diversidade desses delitos, classificação que evolui junto ao desenvolvimento tecnológico e das práticas delituosas. O combate dos crimes informáticos envolve não apenas a aplicação da lei, mas também a cooperação entre governos, empresas, organizações internacionais e a sociedade.

2.3.1 Golpes Informáticos nas Relações Consumeristas

Na atualidade, a internet se transformou em um espaço onde os usuários compartilham informações sobre suas vidas, por meio de redes sociais, transações bancárias via aplicativos, downloads, envio de e-mails, cadastros em sites e outros diversos cliques ao longo de suas navegações. No entanto, após a realização desses procedimentos na rede, o usuário perde o controle sobre o destino e a propagação das informações fornecidas. Esses conteúdos podem ser alterados ou interpretados de maneiras diversas, tornando-se crucial a intervenção do Estado para reprimir os ilícitos e prevenir a sociedade dos perigos presentes no universo cibernético (SILVA, 2017).

Segundo Garcia (2016), diversos termos têm sido empregados na literatura para descrever o comportamento delituoso relacionado a computadores, tais como: ciber criminalidade (*computer-related* crime), crime cibernético (cybercrime), crime tecnológico (*technological crime*), crime assistido por computador (*computer-assisted crime*), crimes digitais (*digital crime*), crimes eletrônicos (*electronic crime*) e crime da Internet (*Internet crime*).

Conforme Almeida et al. (2015), a cibernética é definida como a ciência que estuda os sistemas informantes, especialmente os sistemas de informação. Com base no conceito analítico de crime, as referidas autoras concluem que os "crimes cibernéticos" são todas as ações que se enquadram nos critérios de tipicidade, ilicitude e culpabilidade e que são praticadas contra ou com o uso dos sistemas de informática.

Jesus e Milagres (2016) compreendem que os crimes virtuais se caracterizam como condutas típicas e ilícitas praticadas por meio da tecnologia da informação, ou ainda, contra ela, ou seja, um ato ilícito cometido por meio de informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Para Garcia (2016), um traço comum entre essas definições é a utilização indevida de dispositivos tecnológicos por indivíduos, grupos ou organizações que detêm conhecimentos avançados na área de Tecnologia da Informação.

Horbylon (2022) amplia o conceito de crimes virtuais, destacando que eles podem envolver uma pluralidade de sujeitos. Por exemplo, um hacker que é contratado para roubar informações corporativas de um concorrente pode usar seu conhecimento em explorar falhas de segurança em um sistema. Nesse caso, além do contratante, do hacker e da vítima (concorrente), outros sujeitos podem estar envolvidos.

No que se refere à natureza jurídica dos crimes cibernéticos, Orrigo e Figueira (2015) mencionam a existência de diversas classificações doutrinárias. Os crimes cibernéticos próprios, por exemplo, são aqueles em que o uso do computador é essencial para a sua prática, ou seja, o agente precisa do computador para cometer o delito, e os bens jurídicos afetados pelos crimes cibernéticos próprios são os dados que estão armazenados em outros sistemas ou redes.

Já uma outra categoria, conhecida como crimes virtuais impróprio, é conceituada por Lima (2021) como condutas típicas, antijurídicas e culpáveis que são cometidas por meio de ferramentas informáticas, mas que poderiam ter sido praticadas por outros meios. Coelho e Branco (2016) aprofundam esse conceito, destacando que dentro dessa categoria encontram-se crimes comuns do cotidiano, como é o caso do discurso de ódio na internet, que tem desafiado o equilíbrio entre o direito constitucional à liberdade de expressão e a proteção de direitos fundamentais, como a honra, a imagem, a privacidade e a intimidade. É fundamental ponderar esses direitos em cada caso concreto.

Entretanto, segundo Marra (2019), há ainda três outras categorias de crimes cibernéticos, que são o crime informático puro, o crime de informática misto e o

crime informático comum. O crime informático puro diz respeito ao dano causado diretamente ao sistema de informática, em que o agente busca corromper os dados do computador da vítima, através de vírus e outros meios similares. O crime de informática misto, por sua vez, ocorre quando a violação do bem jurídico lesado não está diretamente ligada ao sistema de informática, mas este é um instrumento necessário para a prática do delito, como acontece no caso de furto eletrônico de contas bancárias. Por fim, o crime informático comum é aquele que já está previsto na lei penal, podendo ou não ser cometido através do uso do computador, como é o caso de crimes como pedofilia, racismo e cyberbullying.

Quanto à classificação dos sujeitos que praticam esses atos, Viana (2001 apud Cruz; Rodrigues, 2018) os dividiu em seis categorias, sendo elas: 1)Crackers de sistemas, que são piratas que invadem computadores conectados em rede; 2) *Crackers* de programas, que quebram proteções de software fornecidos como demonstração para usá-los indefinidamente, como se fossem cópias legítimas; 3) *Phreakers*, que são especialistas em telefonia móvel ou fixa; 4) Desenvolvedores de vírus, *wormse* trojans, que são programadores que criam pequenos softwares que podem causar danos ao usuário; 5)Piratas de programas, que clonam programas, infringindo os direitos autorais; e 6)Distribuidores de *warez*, que são webmasters que disponibilizam softwares em suas páginas sem autorização dos detentores dos direitos autorais.

Em relação às motivações, o autor supracitado apresenta oito tipos de agentes que atuam no ciberespaço. Em primeiro lugar, temos os curiosos, que são aqueles que agem por curiosidade e sem intenção de causar danos à vítima. Eles apenas acessam e leem os dados armazenados, sem modificá-los ou apagá-los. Em segundo lugar, temos os pichadores digitais, que buscam reconhecimento no universo cyberpunk, alterando páginas da internet com seus pseudônimos. O terceiro tipo é o dos revanchistas, funcionários ou ex-funcionários que sabotam a empresa por vingança, aproveitando-se de seu conhecimento sobre as fragilidades do sistema. O quarto tipo é o dos vândalos, que agem pelo simples prazer de causar danos à vítima, podendo chegar à destruição total dos dados armazenados. O quinto tipo é o dos espiões, que procuram obter informações confidenciais armazenadas no

computador da vítima. O sexto tipo são os ciberterroristas, que utilizam várias armas para causar danos, geralmente motivados por questões políticas. O sétimo tipo são os ladrões, que possuem objetivos financeiros claros e frequentemente atacam bancos para desviar dinheiro para suas contas. Por fim, tem-se os estelionatários, que buscam adquirir números de cartões de crédito armazenados em grandes sites comerciais (Viana, 2001 apud Cruz; Rodrigues, 2018).

Além destes, Cruz e Rodrigues (2018) ainda acrescentam as categorias de pedófilos, que buscam crianças na puberdade na internet, e intimidadores, que constrangem, intimidam e ameaçam por meio de sites e redes sociais.

Em face da escassez de informações e da falta de preparo técnico em relação aos contratos de consumo celebrados, os consumidores virtuais estão expostos à vulnerabilidade, não apenas no âmbito das relações materiais inerentes à compra de produtos ou serviços convencionais, mas, sobretudo, diante das empresas virtuais e indivíduos mal-intencionados que se aproveitam da plataforma digital para praticar fraudes e fazer uso indevido de dados desprotegidos pelos fornecedores (Lehfeld et al., 2021). Conforme apontam os autores, a intensificação desse estado de fragilidade tem sido amplamente reconhecida em razão de diversos contratos de adesão que impõem a obrigação de compartilhamento de informações pessoais e outros dados sensíveis, o que tem motivado a criação de mecanismos de proteção adicionais ao Código de Defesa do Consumidor (CDC).

Entretanto, mesmo com tantas práticas criminosas, cenários de vulnerabilidade e a evolução acelerada da internet, até o ano de 2012, não havia legislação específica para punir os crimes cibernéticos, apenas leis que tratavam de crimes cometidos por meio da internet (Bortot, 2017). Contudo, informa a autora, em virtude de alguns episódios, como ataques distribuídos de negação de serviço a sites governamentais e a publicação de fotos íntimas da atriz Carolina Dieckmann, duas leis foram aprovadas com urgência para corrigir algumas das deficiências existentes no ordenamento jurídico sobre o tema: a Lei n°12.735, de 30 de novembro de 2012, conhecida como "Lei Azeredo", e a Lei n°12.737 de 30 de novembro de 2012, conhecida como "Lei Carolina Dieckmann".

A rede mundial de computadores é um ambiente onde as pessoas partilham dados sobre suas existências, realizam operações bancárias por meio de softwares, trocam correspondências eletrônicas, fazem inscrições em páginas da internet e clicam em várias outras coisas durante suas navegações, sem ter total domínio sobre como essas informações serão usadas e espalhadas. Nessa perspectiva, torna-se imprescindível a intervenção das autoridades governamentais para coibir as condutas ilícitas e prevenir a sociedade dos riscos existentes no universo virtual. Desse modo, o capítulo seguinte buscou discutir sobre as implicações jurídicas dos delitos cometidos no âmbito virtual nas relações de consumo, compreendendo tanto as obrigações e responsabilidades das empresas quanto dos consumidores, analisando as medidas de proteção estabelecidas.

2.3.2 Roubo de identidade

O roubo de identidade é uma prática criminosa que envolve a obtenção e uso indevido das informações pessoais de uma pessoa, com o objetivo de cometer fraudes e obter ganhos ilícitos. Essa forma de fraude pode ter graves consequências para as vítimas, incluindo danos financeiros, perda de reputação e estresse emocional. Para Fumagalli, et al., (2016, p.14):

> O roubo de identidade é um crime sofisticado que envolve a obtenção e uso não autorizado de informações pessoais de indivíduos para realizar atividades fraudulentas. Os criminosos exploram vulnerabilidades em sistemas de segurança e técnicas de engenharia social para obter acesso a dados confidenciais. O roubo de identidade pode resultar em consequências financeiras e emocionais significativas para as vítimas, bem como danos à reputação e dificuldades na recuperação de suas identidades.

Fumagalli, et al., (2016), no contexto das fintechs, o roubo de identidade representa um desafio significativo, pois essas instituições lidam com uma quantidade considerável de informações pessoais e financeiras dos clientes. Os fraudadores podem obter acesso a essas informações por meio de técnicas como *phishing*, *malware*, *hacking* e interceptação de comunicações.

Uma vez que os fraudadores tenham obtido as informações de identidade de uma pessoa, eles podem realizar uma série de atividades fraudulentas, como abrir contas bancárias, solicitar empréstimos, fazer compras e realizar transações

financeiras em nome da vítima. Essas ações podem resultar em prejuízos financeiros significativos para as vítimas, além de danos à sua reputação.

O roubo de identidade é uma forma de fraude em que indivíduos utilizam informações pessoais de outras pessoas, como nome, número de Seguro Social e dados financeiros, para obter benefícios financeiros ou cometer crimes. Os criminosos especializados nesse tipo de fraude são conhecidos como "con artistas" profissionais e empregam táticas enganosas para obter as informações necessárias. O roubo de identidade é uma preocupação crescente em nossa sociedade, exigindo maior conscientização e medidas de segurança para proteger as informações pessoais dos indivíduos (Pontell, 2014).

2.4 Competência e territorialidade

É um grande desafio a definição de competência dentro do tema “crimes informáticos”, devido à natureza transacional das tecnologias. O meio digital é um campo muito vasto, por exemplo, um dado inserido na internet pode ser acessado em diversas partes do mundo. O que dificulta a identificação de qual jurisdição tem a competência para julgar as ilegalidades. A Constituição Federal de 1988 configura a repartição de competências:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: LIII - ninguém será processado nem sentenciado senão pela autoridade competente.

Nesse mesmo sentido, o artigo 69 do Código de Processo Penal, determina a competência jurisdicional dos crimes, como sendo o lugar da infração pelo domicílio ou residência do réu; pela natureza da infração; distribuição, conexão ou continência; prevenção ou prerrogativa de função. Restando evidente que a competência é determinada pelo local onde o crime ocorreu, onde o suspeito reside ou onde os servidores e sistemas afetados estão localizados.

Diante disso, a teoria adotada na competência dos crimes informáticos é a teoria do resultado que se concentra nos danos e prejuízos causados pelo uso

indevido das tecnologias. Para reforçar a teoria, o artigo 70 do mesmo código, em seu caput, institui que:

> Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.

Sendo assim, nos os crimes contra a honra, a competência será definida pelo local da consumação do crime, enquanto aos crimes que despeitam a privacidade ou violam o patrimônio a competência será da Justiça Federal.

3 UMA ANÁLISE DAS ESPÉCIES DE CRIMES INFORMÁTICOS

No ambiente virtual, muitas vezes se instaura certa sensação de impunidade diante do anonimato e da dificuldade em se identificar os infratores. O possibilita o surgimento de novas modalidades e técnicas utilizadas para cometer delitos na Internet. Alguns dos principais crimes cometidos no meio informático são a invasão de dispositivos, o estelionato, a pedofilia online, ameaça, cyberbullying e os crimes contra honra.

3.1 A Lei Carolina Dieckmann

A Lei Carolina Dieckmann, oficialmente conhecida como Lei nº 12.737/2012, é uma legislação brasileira que trata especificamente dos crimes cibernéticos, a lei foi criada diante do ocorrido a atriz Carolina Dieckmann. No qual, a atriz teve suas fotos íntimas divulgadas na internet depois de terem roubado e invadido o seu computador. Sendo uma das principais e primeiras medidas tomadas em razão da proteção da privacidade das pessoas no meio digital, a lei foi criada com base no PL 2793/2011. Um dos fundamentos para a proposta:

> São inegáveis os avanços para a sociedade decorrentes do uso da Internet e das novas tecnologias. Estes avanços trazem a necessidade da regulamentação de aspectos relativos à sociedade da informação, com o intuito de assegurar os direitos dos cidadãos e garantir que a utilização destas tecnologias possa ser potencializada em seus efeitos positivos e minimizada em seus impactos negativos. Nesta discussão, ganha relevo constante, sendo objeto de amplos debates sociais, a temática da repressão criminal a condutas indesejadas praticadas por estes meios.

Esta lei estabelece as penalidades para invasão de dispositivos informáticos, interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, além de prever punições para a divulgação ou facilitação de acesso a dados pessoais sem autorização do titular.

Neste contexto, a lei nº 12.737/12, traz algumas alterações no Código Penal brasileiro, sendo elas a tipificação do crime de invasão de dispositivo informático, no artigo 154:

> Invasão de dispositivo informático
>
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou 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 .
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a 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:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4º Na hipótese do § 3º , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal;
>
> - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

> - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

Da mesma forma prevê em seu artigo 154-B do Código Penal Brasileiro, que os crimes de invasão de dispositivo informático serão de ação pública condicionada a representação; ressalvado se o crime for cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. A partir dessa lei o país passou a ampliar os meios de prevenção aos delitos cometidos ambiente digital.

3.2 Pedofilia online

A pedofilia não está tipificada no ordenamento jurídico brasileiro como crime, por se tratar de uma doença psicológica. Porém existem várias leis que tratam do assunto. Um dos exemplos, é a Lei nº 8.069, de 13 de julho de 1990, denominada O Estatuto da Criança e do Adolescente (ECA), que dispõe medidas de proteção e punições para crimes contra crianças e adolescentes no Brasil. O Artigo 241 do ECA, institui que:

> Art. 241 Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.

Da mesma forma em seus artigos 241-A até 241-E, criminaliza a produção, distribuição, facilitação, divulgação e obtenção de material pornográfico envolvendo crianças e adolescentes. Com a pena podendo variar de acordo com a gravidade e circunstâncias do crime, mas geralmente envolvem a reclusão e multas.

Além das leis específicas, as autoridades brasileiras têm intensificado esforços para combater a pedofilia online, através de operações policiais especializadas e cooperação internacional para investigação e punição de criminosos envolvidos nesses delitos.

A internet atualmente é um meio disponível a qualquer um que tenham acesso a um celular, tablet ou computador, as crianças, por exemplo, começam desde cedo a serem expostas a tecnologia, muitas vezes o acesso é desacompanhado dos

pais ou responsáveis. O que dá abertura e atrai pessoas mal-intencionadas como os pedófilos, possam se aproximar virtualmente desses menores, podendo até mesmo marcarem encontros em áreas isoladas para dificultar a descoberta do crime.

3.3 Os crimes contra a honra

No contexto online, os crimes contra honra muitas vezes se manifestam através da calúnia, injúria e difamação. Os meios mais propícios para o cometimento dos crimes são as redes sociais, fóruns online e mensagens eletrônicas. São crimes em que o bem tutelado é a honra, sendo que os agressores usam do escárnio e da humilhação para desqualificar a vítima. Nesse caso, as vítimas podem sofrer consequências devastadoras, tanto na vida pessoal como na profissional. Nesse sentido:

> Outra modalidade de delito tipificado no código incriminador que se adequa aos chamados crimes cibernéticos impróprios, diz respeito aos crimes que tem por objetivo tutelar o bem jurídico honra. Calúnia, difamação e injúria, crimes contra a honra elencados respectivamente nos artigos 138, 139 e 140 do Código Penal, são infrações que ganharam maior amplitude, através da utilização de ferramentas
>
> informáticas como as mídias sociais, blogs, sites, aplicativos de comunicação, dentre outros, que facilitam e dinamizam o cometimento desses ilícitos. (Matsuyama e Lima, 2017, p.7).

A Constituição da República Federativa do Brasil que institui a maiorias dos direitos fundamentais, em seu artigo 5º dispõe que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. O que garante que o direito a honra é um direito fundamental protegido pelo nosso ordenamento jurídico.

Aduz Bettencourt (2011, p.314) que João Batista de Menezes Bittencourt, que independe de qualquer que seja a definição dada a honra, ela é um interesse penalmente protegido. É importante, do ponto de vista de o amparo penal à honra, pois “ela não diz respeito apenas ao interesse exclusivo do indivíduo, mas também da coletividade, que tem interesse na preservação da honra, da incolumidade moral e da intimidade além de outros bens jurídicos indispensáveis para a harmonia social”.

É necessário esclarecer adequadamente os significados dos crimes de calúnia, difamação e injúria, especialmente porque na percepção popular esses termos podem ser considerados sinônimos.

Os crimes contra a honra estão previstos respectivamente nos artigos 138, 139 e 140 do Código Penal Brasileiro. A calúnia consiste em imputar a alguém fato que constitua crime. Por exemplo, acusar alguém de um crime, sem ter provas que comprove sua afirmação. A difamação refere-se a uma declaração falsa que prejudica a reputação de alguém, nesse caso, são apresentadas afirmações verdadeiras, mas ditas de uma maneira que prejudique a reputação da pessoa. E a injúria refere-se a ofensa seja verbal ou escrita feita a outrem que atinge a dignidade ou respeito de uma pessoa.

Em suma, cada um desses crimes tem suas próprias características, apesar envolver danos à reputação de uma pessoa, se distinguem tanto na aplicação legal quanto em suas implicações.

3.4 Cyberbullying

Com o advento da Internet as relações pessoais adquiriram um novo contexto, atualmente uns dos prazeres humanos são os de postar, publicar e falar de sobre tudo e todos na rede mundial de computadores. A onda de bullying é crescente e com ela a sensação de impunidade que proporcionada pela internet.

O crime de cyberbullying, uma derivação do bullying tradicional, envolve atos de violência psicológica, humilhação, xingamentos e outras formas de intimidação, realizados no ambiente digital. Assim como o bullying, o cyberbullying pode ter graves consequências para as vítimas. A pressão constante pode levar a uma baixa autoestima, ansiedade e até mesmo traços de depressão, aumentando o risco de autoagressão e suicídio.

Nesse pensamento, Francisco Porfírio, constata que:

> Assim como ocorre com o bullying praticado fora do ambiente virtual, o cyberbullying pode ter sérias consequências para os jovens vitimados. Em geral, um quadro inicial de isolamento e tristeza pode evoluir para sérios quadros de depressão, transtorno

> de ansiedade e síndrome do pânico. Se o caso não for descoberto e as sequelas não forem tratadas, as vítimas de cyberbullying podem carregar consigo sintomas de trauma pelo resto de suas vidas, o que provoca, muitas vezes, baixo desempenho escolar, baixa autoestima, dificuldades em se relacionar com os outros e se colocar no mercado de trabalho quando na vida adulta, além de problemas da busca de alívio dos problemas nas drogas e no álcool. Nos casos mais extremos, a vítima de cyberbullying pode cometer suicídio.

As consequências do cyberbullying são inúmeras, podendo causar danos sociais, emocionais, nesses casos pode gerar baixa autoestima, ansiedade, depressão como diversos outros problemas emocionais, de comportamento e diversos outros. Além disso, o cyberbullying afeta não apenas os indivíduos diretamente envolvidos, mas também suas famílias, amigos e comunidades.

3.5 Estelionato

O crime de estelionato, busca a punição do indivíduo que obtém vantagem indevida sobre outrem, causando-lhe prejuízo, previsto no Código Penal Brasileiro em seu artigo 171, descreve estelionato como:

> "Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis."

No mesmo sentido, define Assunção (2021):

> Tratando-se do crime de estelionato no ambiente da internet, o sujeito ativo mantém a vítima em erro, sob a finalidade de obter vantagem ilícita para si próprio. Também considera-se crime cibernético exaltar ou elogiar criminoso ou ato criminoso de maneira pública, caracterizando crime de apologia de crime ou de criminoso. (Assunção, 2021, p.8).

Sendo um dos crimes de maior incidência no Brasil, segundo o Fórum Brasileiro de Segurança Pública, o Brasil que registrou uma média de 208 golpes por hora e chegando a 1,8 milhões em 2022. O que equivale a um aumento de 368,3% em relação a 2018.

No estelionato, são criadas diversas formas como, e-mails e sites fraudulentos para que se obtenha vantagem indevida sobre as vítimas, em sua grande maioria com o objetivo de conseguir dinheiro em troca. O objetivo principal

desse crime é proteger o patrimônio das vítimas de condutas fraudulentas praticadas contra elas.

É fundamental estabelecer punições para esse delito e efetiva aplicação da lei, para que a prática seja desencorajada e haja proteção do patrimônio e a segurança de toda a sociedade.

3.6 A Lei Nº 13.709 DE 14 de agosto de 2018

A Lei Geral de Proteção de Dados (LGPD) regulamenta o tratamento de dados pessoais e no meio de digital, como também traz sanções administrativas para prevenir o vazamento de dados pessoais.

Para definição de dados pessoais, a lei traz em seu artigo 5º que: I - dado pessoal: informação relacionada à pessoa natural identificada ou identificável; nesse caso, podendo incluir como meios de identificação nome, endereço, número de identificação, informações de contato, informações médicas, dados biométricos, histórico de compras, preferências pessoais, entre outros. Além de preservar informações pessoas, também garante a segurança e dificulta a obtenção de informações por criminosos.

As punições para quem despeita essa lei são graves, ficando sujeitos a sanções administrativas, dispostas no artigo 52 da lei dentre elas a pena de advertência, com indicação de prazo para adoção de medidas corretivas, a pena de multa, entre outras que tem por objetivo fazer com que as medidas de segurança sejam mais rígidas e eficazes.

Os artigos 11 aos 13 da lei evidenciam a necessidade de um rigor maior na proteção dos dados pessoais. De acordo com o artigo 5º, inciso II, da LGPD, esses dados são definidos como aqueles que, por sua natureza, demandam um tratamento ainda mais cauteloso, o doutrinador define:

> Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

A primeira empresa a ser condenada por violar a LGPD, foi a Cyrela, uma grande empresa no ramo imobiliário que vazou dados pessoais de um cliente sem a autorização após a compra de um imóvel em 2018, foi condenada pela justiça de São Paulo a pagar R$10.000,00 de indenização (Lima, 2022, online).

Esse vazamento de dados é uma clara violação à Lei Geral de Proteção de Dados e que fomenta a necessidade de consentimento no uso de dados pessoais de outrem. Além disso, o caso serve de aviso para as demais empresas, sobre a segurança que elas proporcionam no uso de dados em políticas e procedimentos eficazes de proteção de dados, não apenas para evitar penalidades legais, mas também para proteger a confiança e a reputação de seus clientes.

A LGPD se tornou um marco importante no contexto da revolução digital, representando a regulamentação e proteção da privacidade dos cidadãos brasileiros.

4 AS FERRAMENTAS DE PREVENÇÃO E REPRESSÃO AOS CRIMES INFORMÁTICOS

Entretanto, mesmo com tantas práticas criminosas, cenários de vulnerabilidade e a evolução acelerada da internet, até o ano de 2012, não havia legislação específica para punir os crimes cibernéticos, apenas leis que tratavam de crimes cometidos por meio da internet (BORTOT, 2017). Contudo, informa a autora, em virtude de alguns episódios, como ataques distribuídos de negação de serviço a sites governamentais e a publicação de fotos íntimas da atriz Carolina Dieckmann, duas leis foram aprovadas com urgência para corrigir algumas das deficiências existentes no ordenamento jurídico sobre o tema: a Lei n°12.735, de 30 de novembro de 2012, conhecida como "Lei Azeredo", e a Lei n°12.737 de 30 de novembro de 2012, conhecida como "Lei Carolina Dieckmann

O Direito Penal ainda enfrenta desafios para lidas com os crimes informáticos. A dificuldade se dá no fato de que a tecnologia avança de forma rápida, necessitando que as alterações na legislação sejam rápidas de igual modo, para acompanhar as novas formas de criminalidade.

Os crimes informáticos se tornaram uma ameaça mundial, os crimes tem sido cada vez mais sofisticados e frequentes, representam uma ameaça significativa para organizações e pessoas por todo o mundo. Embora a expressão "a internet é terra sem lei" seja usada frequentemente, a internet não o campo do anonimato uma vez que é possível identificar os indivíduos malfeitores através de investigações organizadas e efetivas.

No contexto do ordenamento jurídico brasileiro, além da legislação específica, qual seja, a Lei nº 12737/12, também conhecida como "Lei Carolina Dieckmann", o Marco Civil da Internet e a Lei Geral de proteção de dados, existem mais mecanismos que possibilitam a prevenção e repressão dos crimes na era digital. Órgãos como a polícia civil e polícia federal possuem unidades em todos os estados para o combate aos delitos cometido no meio digital.

À medida que a tecnologia avança, os criminosos também aprimoram suas técnicas para atingir um grande número de vítimas. É fundamental, portanto, que os crimes estejam associados às ferramentas mais utilizadas pelos usuários. O comércio eletrônico oferece várias oportunidades para indivíduos inescrupulosos obterem vantagem sobre consumidores ingênuos ou desatentos, bem como sobre aqueles com mais experiência, que podem ser enganados pela falsa sensação de segurança que a Internet aparenta oferecer. É importante ressaltar que, mesmo com a implementação de ferramentas virtuais de segurança, é impossível garantir total proteção contra a ação criminosa (Teixeira; Chaves, 2019).

Como descrito anteriormente, as primeiras medidas constitucionais que visavam a proteção de dados digitais no Brasil, ocorreram somente em 2012. Em vista da análise da tipificação penal e do contexto tecnológico em que a sociedade contemporânea se encontra, Duran e Barbosa (2020) compreendem que a inclusão de novas medidas, como é o caso do artigo 154-A, no Código Penal pela Lei 12.737/2012 era fundamental para a resolução dos conflitos que o mundo jurídico não estava previamente preparado para lidar.

A LGPD brasileira preconiza a necessidade de obtenção do consentimento do titular de dados pessoais para que estes sejam recolhidos e tratados, salvo as

exceções previstas no dispositivo legal em questão. Consequentemente, os princípios da privacidade e da transparência são convergentes na rotina de tratamento de dados, visto que a coleta e tratamento de dados pessoais dependem do consentimento do titular, enquanto que os poderes públicos devem promover a divulgação de informações relevantes à sociedade, garantindo a transparência (Barbosa, 2020).

Com a promulgação da Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados, as empresas precisam adequar-se aos novos princípios que regem a regulamentação do direito civil na Internet, enfrentando desafios no processo de mapeamento de dados pessoais, revisão de contratos com fornecedores e consumidores, e mudança de cultura corporativa. Desde que a LGPD entrou em vigor, em agosto de 2020, as empresas tiveram o tempo necessário para se adaptar às novas regras, criando relatórios e manuais a fim de garantir a conformidade com a legislação vigente (Mesquita, 2021).

Conforme Mendes (2017), a proteção de dados pessoais no contexto da regulamentação da internet é essencial para a garantia do exercício dos direitos fundamentais, como a liberdade de expressão e de comunicação. Isso se deve ao fato de que o usuário necessita confiar na segurança da rede para se comunicar e se expressar livremente, o que só é possível com a proteção da privacidade e dos dados pessoais. Caso contrário, se houver a possibilidade de utilização inadequada de seus dados, o usuário agirá com receio no ambiente virtual e não exercerá suas ideias com total liberdade.

Além disso, é fundamental que esses provedores utilizem meios tecnológicos que permitam a correta identificação dos dados de conexão dos ofensores, de modo que tais informações possam ser disponibilizadas ao ofendido. Ainda nesse sentido, cabe aos provedores assumirem a responsabilidade de fornecer os dados necessários para identificação dos ofensores, mas sem expor os dados cadastrais e de conexão de usuários, salvo exceções previstas em contrato ou conforme previsão legal (Costa, 2019).

Embora a Lei Geral de Proteção de Dados (LGPD) esteja mais voltada para a preocupação com dados e coleta, o CDC, por sua vez, parte da premissa de que o consumidor é vulnerável em relação ao poder econômico do fornecedor, o que é uma das bases fundamentais da lei (Pinto; Diniz, 2022).

A legislação relacionada à fraude cibernética em fintechs é composta por um conjunto de leis e normas que visam proteger os usuários e punir os responsáveis por práticas criminosas. Dentre as leis específicas, destacam-se o Código Penal, a Lei de Crimes Cibernéticos e a Lei Geral de Proteção de Dados. No entanto, existem lacunas e desafios enfrentados pelo direito penal brasileiro na efetiva aplicação dessas leis diante das inovações tecnológicas e complexidades das fraudes cibernéticas (Ribeiro,2022).

O combate à fraude cibernética em fintechs no Brasil conta com instrumentos legais específicos. O Código Penal Brasileiro, estabelecido pelo Decreto-Lei nº 2.848/1940, apresenta dispositivos que podem ser aplicados nesse contexto. Por exemplo, os artigos que tratam dos crimes de estelionato (art. 171), falsidade ideológica (art. 299) e acesso indevido a dispositivo informático (art. 154-A) são utilizados para punir indivíduos envolvidos em fraudes cibernéticas.

Portanto, Dholakia e Dholakia (2020), comentam que essas leis fornecem um arcabouço jurídico para a repressão e punição dos crimes cibernéticos, incluindo fraudes em fintechs. É essencial que as instituições financeiras e os usuários estejam cientes dessas legislações e que haja uma efetiva colaboração entre as autoridades, as fintechs e os órgãos reguladores para garantir a aplicação adequada das leis e a proteção dos sistemas financeiros digitais e outros crimes que vem ocorrendo no Brasil.

4.1 Processo de investigação

De acordo com Torres Júnior (2015), a Lei 12.737/12, conhecida como Lei Carolina Dieckman, apresenta falhas ao deixar de tratar de sobre a privacidade dos indivíduos. O autor aponta para a necessidade de ampliação dos mecanismos de proteção da intimidade e privacidade no ambiente virtual, com ênfase na preservação de dados e informações armazenadas na internet. Segundo ele, o artigo

154-A não é suficiente para garantir uma proteção efetiva, e sugere uma reformulação de seu conteúdo ou a criação de novos dispositivos legais, como o Projeto de Lei 5555/2013, que busca preencher as lacunas presentes na Lei Carolina Dieckman.

De acordo com a análise de Carvalho (2017), a legislação vigente apresenta uma restrição aos direitos do usuário que se encontra na posição de vítima, uma vez que não são garantidos de forma imediata seus direitos fundamentais em relação à intimidade e privacidade, em razão da falta de responsabilização direta dos provedores de aplicações da internet pelo art. 19.

Essa autora observa que, ao privilegiar o direito à liberdade de expressão, pode ser identificado um retrocesso, já que existe uma colisão de direitos fundamentais, a saber: a liberdade de expressão, prevista no inciso IV do art. 5º da Constituição Federal, e o direito à privacidade, disposto no inciso X do mesmo artigo 5º, que neste caso é desvalorizado. Em outras palavras, o direito à privacidade e intimidade da vítima é colocado em segundo plano, em detrimento do direito à liberdade de expressão, o que pode gerar um conflito entre esses direitos fundamentais.

A investigação dos delitos online, só começam após a devida denúncia, esse primeiro passo é o mais importante para conhecimento do crime e da tomada das demais providências. O meio pelo qual o delito é cometido tem que ficar da mesma forma identificado, uma vez que, podem ser utilizados e-mails, web sites, redes sociais, salas de bate, dentre outros nesse universo extremamente rico de opções.

No direito processual penal, a obtenção de provas é fundamental para verificar a ocorrência de um crime, em consonância com o princípio da verdade real. Nesse contexto, é de suma importância garantir que os dados presentes no computador utilizado para cometer o delito, bem como nos dispositivos pertencentes à vítima, não sejam apagados.

Para que possamos conviver bem e com harmonia em sociedade, existem órgãos responsáveis pelo controle da segurança no meio. Deste modo, cabe à polícia duas funções distintas: uma de natureza administrativa e outra de natureza

judiciária. Nesse sentido, sua atuação ocorre tanto de forma preventiva quanto repressiva, com o propósito de disciplinar, regulamentar e fiscalizar os direitos e interesses dos cidadãos (Brene; Lepore, 2017). O artigo 144 da Constituição Federal ressalta que:

> Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos:I - polícia federal;II - polícia rodoviária federal;III - polícia ferroviária federal; V - polícias civis; V - polícias militares e corpos de bombeiros militares. VI - polícias penais federal, estaduais e distrital.

A polícia judiciária deve estar plenamente preparada para investigação criminal, especialmente no contexto dos crimes informáticos, onde a expertise em tecnologia da informação e forense digital se torna essencial. É necessário contar com profissionais capacitados e equipamentos adequados para coletar, preservar e analisar evidências digitais, garantindo a eficácia das investigações e a responsabilização dos perpetradores de crimes cibernéticos.

Uma análise forense digital que envolve a coleta e preservação de evidências digitais como computadores, tablets, smartphones, como também desempenha o papel de recuperação de dados, autenticação das evidências, identificação dos criminosos e atividades suspeitas.

É indiscutível que, diante da evolução dos crimes cibernéticos e do progresso das investigações, a especialização dos profissionais se torna uma consideração primordial. Além disso, destaca-se que essa especialização pode ser alcançada por meio da cooperação institucional, através do intercâmbio de informações de investigação e soluções de tecnologia da informação (Silva, 2006).

Ademais, o CDC dispõe, em seu artigo 6º, dos princípios norteadores das relações de consumo, que incluem o direito à segurança, à educação para o consumo, à informação, à proteção contratual e pré-contratual, à indenização e prevenção de danos e à melhoria dos serviços públicos. Portanto, tais princípios visam a assegurar a efetiva proteção dos direitos do consumidor, bem como a prevenção de práticas abusivas no mercado de consumo (BRASIL, 2020).

Dessa maneira, entende-se que o CDC abrange aspectos amplos, como bancos de dados e cadastros de consumidores, no artigo 43, com o intuito de proteger o cidadão diante da desigualdade de poder entre consumidor e fornecedor, assegurando-lhe independência e autonomia para a tomada de decisões comerciais, de maneira prática e concreta, diferente da perspectiva ideológica da LGPD. Assim, é possível verificar que há uma complementaridade entre as duas normativas brasileiras nesse tema (Pinto; Diniz, 2022).

4.2 Educação digital

A educação digital é um componente essencial na formação de cidadãos responsáveis e competentes em um mundo cada vez mais conectado. Em mundo onde a tecnologia faz parte do cotidiano das pessoas, desde o laser até as relações de trabalho é fundamental que desenvolvam noções e habilidades para navegar no meio tecnológico de maneira segura.

A definição da palavra "educar" é derivada do Latim Educare, que significa orientar, conduzir, colaborar com a evolução intelectual do indivíduo, o que possibilita seu convívio no meio social (ETIMOLOGIA, 2019).

Dessa maneira nas escolas e demais instituições de ensino, a educação digital deve fazer parte do currículo acadêmico, abrangendo todas as disciplinas e não só uma de forma isolada. Os alunos devem aprender o uso correto da tecnologia de maneira crítica e reflexiva, desenvolvendo habilidades com discernir entre um conteúdo confiável ou não, utilizar informações confiáveis, entre outros.

O Marco Civil da Internet ou lei nº 12965/2014, estabeleceu a respeito da educação digital, sendo:

> Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.

A criação de políticas públicas também fomenta a educação digital, como destacado no artigo 27, sendo o Estado também responsável ´pela inclusão digital, a

diminuição das desigualdades no acesso às tecnologias, como também a tarefa de fomentar a produção e circulação de conteúdo nacional (BRASIL, 2014, online).

O artigo 28 da mesma lei institui como dever do Estado em formular e fomentar estudos, estratégias, planos e cronogramas para o uso e desenvolvimento da Internet no país (BRASIL, 2014, online).

Além disso, a conscientização sobre os riscos associados ao uso da tecnologia, como o cyberbullying, estelionato, vazamento de dados e dependência tecnológica. A educação digital também desempenha o papel de capacitação dos profissionais para lidar com a proteção e segurança de dados.

Além disso, o artigo 7º, inciso I do Marco Civil estabelece como direito do usuário "a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano moral decorrente de sua violação", dispositivos praticamente idênticos (Tomas e Vicius Filho, 2016).

Para Pinheiro (2016), a evolução tecnológica e o crescente uso da internet fizeram surgir a necessidade de um ramo específico do direito que contemple as particularidades do meio digital, o chamado direito digital. Segundo o autor, a maioria das normas atuais não foi pensada para aplicação no ambiente virtual, o que pode trazer dificuldades na punição de crimes cometidos neste meio. De fato, as normas brasileiras, em sua maioria, não contemplam as especificidades do ambiente digital, o que pode permitir que o agente de um crime eletrônico se esquive da responsabilização, alegando a falta de provas ou argumentando que não foi ele o autor do fato criminoso.

De acordo com o posicionamento do Ministério Público Federal (BRASIL, 2018), em muitos casos, o crime eletrônico é um crime de meio, ou seja, utiliza-se do meio virtual como instrumento para a materialização da conduta delituosa. Porém, nem sempre o crime é exclusivamente virtual, sendo possível enquadrá-lo em outras categorias, como estelionato, extorsão, falsidade ideológica, fraude, entre outros. Dessa forma, é necessário um olhar atento e específico para a aplicação das normas em casos de crimes digitais, a fim de garantir a responsabilização adequada dos autores e a proteção dos direitos dos usuários da internet.

De acordo com Fiorillo e Conte (2017), é notório que os crimes em ambiente digital são recorrentes e facilmente realizados, porém muitas vezes não são investigados nem punidos devido à baixa possibilidade de identificação e punição do autor, uma vez que o ambiente digital permite que o usuário permaneça anônimo.

Além disso, Souza (2020) ressalta que, embora existam especialistas em invasões de dispositivos e outros crimes cibernéticos, como os hackers e crackers, a maior parte dos crimes no meio digital são comuns e direcionados a pessoas, como os crimes contra a honra. É inegável que a complexidade em identificar a autoria de um crime no meio digital ainda proporciona margem para que o agente criminoso conteste a autoria, alegando que sua conta foi indevidamente invadida ou que um usuário com seu nome não é ele, como aponta o Ministério Público.

Referente ao CDC, Rezende e Paula (2021), entendem que, no presente momento, a legislação se apresenta incompleta, o que gera a percepção de sua inacababilidade em face das constantes mudanças do mundo. Em matéria de relação entre fornecedor e consumidor, é imperioso que se dê primazia ao princípio da vulnerabilidade do consumidor, que se encontra em posição de fragilidade no processo e, por conseguinte, merecedor de maior proteção jurídica.

Para Teixeira (2015), um dos maiores desafios para o CDC é a falta de regulação específica para o comércio eletrônico. Muitos dos crimes virtuais ocorrem em plataformas online, como sites de compras e redes sociais, que não estão sujeitas às mesmas regras e fiscalização que as lojas físicas. Isso dificulta a aplicação do CDC, que muitas vezes não é adequado para lidar com as particularidades do ambiente virtual.

Outra questão é a dificuldade de identificar e responsabilizar os autores de crimes virtuais. Muitas vezes, esses indivíduos se escondem atrás de pseudônimos e usam técnicas de criptografia para evitar serem rastreados (Barros, 2021). Esses pseudônimos são utilizados como uma forma de ocultar a verdadeira identidade dos criminosos, tornando mais difícil sua localização e identificação. Além disso, muitos criminosos utilizam técnicas de falsificação de identidade, criando perfis falsos em redes sociais e sites de comércio eletrônico para enganar os consumidores.

Já a criptografia, técnica amplamente utilizada pelos criminosos virtuais para evitar serem rastreados, é um método de codificação de informações, que torna as informações ilegíveis para quem não tem acesso à chave de decodificação. Dessa forma, os criminosos podem realizar suas atividades ilegais sem serem detectados, pois suas atividades são protegidas por uma camada de criptografia (Pacífico; Gomes, 2021)

Outro problema relacionado à eficácia do CDC frente às práticas de crimes virtuais é a falta de atualização da legislação. Segundo Silva (2020), o CDC foi criado em 1990, em um momento em que a internet ainda não era uma realidade acessível para a maioria das pessoas. Com o avanço da tecnologia, novas práticas criminosas surgiram, tornando necessária a atualização constante da legislação para garantir a proteção do consumidor.

Ainda segundo Silva (2020), a dificuldade de acesso à justiça é outro problema enfrentado pelos consumidores vítimas de crimes virtuais. Muitas vezes, as vítimas não sabem como proceder para denunciar os crimes ou não possuem recursos para contratar advogados especializados. Além disso, muitas empresas de tecnologia não possuem sede no Brasil, o que dificulta a aplicação da legislação brasileira.

Além disso, para Chagas (2023), outro ponto que afeta a eficácia do CDC frente aos crimes virtuais é a falta de conscientização dos consumidores. Muitas pessoas não têm conhecimento dos riscos envolvidos nas transações online e não adotam medidas de precaução para se protegerem. Isso pode levar a situações em que o consumidor é lesado, mas não tem como provar que o dano foi causado por uma prática ilegal.

Todas essas táticas dificultam a identificação e responsabilização dos autores de crimes virtuais, tornando o trabalho das autoridades e instituições encarregadas de combater essas práticas ainda mais desafiador. É preciso investir em tecnologia e capacitação para lidar com essa complexa e em constante evolução realidade, buscando cada vez mais meios eficientes para a identificação e responsabilização dos criminosos virtuais (Vieira et al., 2022).

Por fim, é importante destacar que a proteção do consumidor no ambiente virtual não depende apenas do CDC brasileiro, mas também da atuação conjunta das empresas de tecnologia, das autoridades brasileiras e dos próprios consumidores. É preciso investir em tecnologia e educação para lidar com essa realidade em constante evolução, buscando sempre novos meios para garantir a proteção dos consumidores no ambiente virtual (RODRIGUES 2021).

5 A PROTEÇÃO DO CYBERCONSUMIDOR NO ORDENAMENTO JURÍDICO BRASILEIRO

Dentro das normas de Direito, se apresenta um desafio à proteção do cyberconsumidor, que diz respeito ao consumidor utilizando-se da internet, delimitando-se em diversas problemáticas que circundam o tema, tais como a responsabilidade civil dos estabelecimentos virtuais, e a confiabilidade dos consumidores diante todos os riscos. Mesmo com todas as normas e proteções que emanam do Código de Defesa do Consumidor - CDC, este contém lacunas quanto a esses novos métodos e meios de consumo, o qual na sua época de criação não existia a expressiva demanda no mercado digital, precisando, portanto, a adequação das leis existentes ou criação de novas leis.

O Código de Defesa do Consumidor define, em seu artigo 6º, os chamados "direitos básicos" dos consumidores. Dentre eles, destacam-se aqui, de forma especial, aqueles insertos em seus incisos III (informação), IV (proteção contra abusos de toda sorte, nas diversas fases da relação de consumo) e VI (efetiva prevenção e reparação de danos morais) (BRASIL, 1988).

Tem-se que o atual CDC é perfeitamente aplicável às relações consumeristas no meio virtual. Porém, mesmo que possam ser estendidas ao comércio eletrônico, as tratativas elencadas no CDC fazem menção apenas às relações de consumo realizadas fisicamente, quando as partes estão presentes ou ainda, quando entre ausentes, mas havendo conhecimento da localização das partes e possíveis encontros futuros para acertar o negócio realizado.

Por esta razão, o CDC irá passar por uma alteração, a qual é tratada no Anteprojeto de Atualização do Código de Defesa do Consumidor, a fim de embarcar

na proteção oferecida por este os também consumidores eletrônicos e as relações virtuais de consumo, sejam elas via e-mail, sites ou telefone (Finkelstein, 2011).

Essa legislação teve origem no Projeto de Lei do Senado Federal nº 283/2012, que propôs modificações na Lei nº 8.078, de 11 de setembro de 1990, conhecida como Código de Defesa do Consumidor, e no art. 96 da Lei nº 10.741, de 1º de outubro de 2003, também conhecida como Estatuto do Idoso, com o objetivo de aprimorar a regulamentação do crédito ao consumidor e abordar questões relacionadas ao superendividamento. Esse projeto foi elaborado por uma comissão composta por juristas especializados nesse tema.

No dia 4 de novembro de 2015, o projeto foi recebido pela Câmara dos Deputados e passou pelas Comissões de Defesa do Consumidor, Finanças e Tributação, além da Comissão de Constituição e Justiça e de Cidadania. A partir de 2019, o projeto passou a tramitar em regime de prioridade, e uma Comissão Especial foi criada com o objetivo de emitir parecer sobre o PL nº 3.515/2015 e suas apensas. Já no dia 3 de setembro de 2019, a Comissão Especial foi estabelecida, tendo a Deputada Mariana Carvalho como Presidente e o Deputado Franco Cartafina como relator. Devido à importância do tema, o projeto foi submetido a votação e aprovado pelo plenário em 11 de maio de 2021 (Borges, 2021).

No âmbito do comércio eletrônico, segundo informações do portal de notícias do Senado, denominado Agência Senado (AS, 2012), destacam-se propostas relevantes que visam regular esta modalidade de comércio de forma específica. Dentre elas, destaca-se a proposta de criar uma nova seção no CDC que se dedicará ao tratamento adequado do comércio eletrônico. Tal medida tem o objetivo de garantir que as informações pertinentes à identificação do fornecedor, incluindo seu endereço geográfico, sejam disponibilizadas de maneira destacada e de fácil visualização. Ademais, é assegurado ao consumidor o direito de receber a confirmação da transação e de corrigir eventuais equívocos presentes nos contratos realizados à distância (BRASIL, 2021).

Outra proposta relevante consiste na proibição do envio de spam e mensagens eletrônicas não solicitadas pelos fornecedores de produtos e serviços

aos consumidores com os quais não possuam relação de consumo prévia, bem como àqueles que manifestaram expressamente sua recusa ou estão registrados em cadastros de bloqueio (BRASIL, 2021).

Em relação ao exercício do direito de arrependimento nos contratos celebrados à distância, propõe-se o reforço e a facilitação desse direito, permitindo ao consumidor exercê-lo dentro do prazo de sete dias (BRASIL, 2021).

No que tange às práticas abusivas por parte dos fornecedores contra os consumidores, propõe-se a introdução de penalidades que incluem a suspensão e a proibição do uso do comércio eletrônico por parte desses fornecedores reincidentes. Adicionalmente, caso ocorra o descumprimento das penalidades, o juiz poderá determinar o bloqueio das contas bancárias do fornecedor infrator, assim como a suspensão dos repasses de pagamentos e transferências financeiras, com o intuito de compelir o cumprimento das sanções impostas (BRASIL, 2021).

No âmbito do superendividamento do consumidor, destacam-se medidas relevantes. Uma delas consiste na proibição da veiculação de publicidade de crédito que faça referência a expressões como "crédito gratuito", "sem juros", "sem acréscimo", com taxa zero ou de sentido semelhante (BRASIL, 2021).

Com o objetivo de prevenir o superendividamento, propõe-se a adoção da concessão responsável de crédito, que exige que os fornecedores, além de fornecer informações, também aconselhem o consumidor e avaliem, de maneira justa, sua capacidade de pagamento das dívidas. O descumprimento dessas obrigações acarretará na redução dos juros incidentes (BRASIL, 2021).

Outra medida importante é a instituição do conceito de assédio de consumo, que se caracteriza pela pressão exercida sobre o consumidor, especialmente se este for idoso, analfabeto, doente ou estiver em situação de vulnerabilidade agravada, com o intuito de induzi-lo a contratar produtos, serviços ou crédito, principalmente quando realizado de forma remota, por meio eletrônico ou telefônico, ou quando envolver benefícios ou prêmios (BRASIL, 2021).

Por fim, propõe-se a criação do procedimento intitulado "da conciliação em caso de superendividamento", que visa estimular a renegociação das dívidas dos consumidores em audiências conciliatórias com todos os credores. Nesse procedimento, elabora-se um plano de pagamento com prazo de até cinco anos para a quitação das dívidas, respeitando o mínimo existencial.

Para tanto, o legislador brasileiro busca agora regular as relações virtuais consumeristas, a fim de suprir a lacuna quanto ao Comércio Virtual revisando alguns artigos da Lei 8.079/90 (Código de Defesa do Consumidor - CDC).

Verifica-se que o objetivo da atualização é ampliar a proteção ao e-consumer e adaptar o CDC aos novos métodos aplicados ao comércio em âmbito eletrônico, seja na questão de direitos referentes ao cyberconsumidor, seja quanto aos deveres dos fornecedores virtuais. Tendo isto em mente, vislumbra-se que se busca minimizar a vulnerabilidade do consumidor que, na internet, torna-se ainda mais hipossuficiente frente ao fornecedor, pois a compra em meio eletrônico ocorre na maioria das vezes “às cegas” por não conhecer quem está do outro lado da relação jurídica.

5.1 O Direito Penal e os Crimes Informáticos

Na era digital, o avanço rápido da tecnologia tem trazido inúmeros benefícios para a sociedade, mas também novos desafios, especialmente no campo da segurança cibernética. Com a proliferação da internet e dos dispositivos conectados, os crimes informáticos se tornaram uma preocupação central para legisladores, autoridades de segurança e cidadãos (Cavalcanti, 2024).

O Direito Penal, como ramo jurídico responsável por estabelecer as condutas consideradas criminosas e suas respectivas penas, desempenha um papel crucial na prevenção e repressão desses delitos. Este capítulo analisa as ferramentas legais e tecnológicas utilizadas no combate aos crimes informáticos, abordando sua eficácia e os desafios enfrentados na implementação dessas medidas (Gomes, 2023).

No âmbito tecnológico, a implementação de sistemas de segurança robustos, como firewalls, antivírus e ferramentas de criptografia, é essencial para prevenir

ataques cibernéticos. As empresas e instituições devem investir em infraestrutura de segurança, realizar auditorias periódicas e treinar seus funcionários para reconhecer e reagir adequadamente a ameaças cibernéticas. A conscientização dos usuários finais também é uma ferramenta preventiva vital. Campanhas de educação digital podem ensinar os consumidores a adotar práticas seguras, como a utilização de senhas fortes e a evitação de links suspeitos (Ferreira, 2023).

A repressão aos crimes informáticos envolve a aplicação rigorosa das leis penais e a utilização de tecnologias avançadas para investigar e punir os responsáveis por essas atividades ilícitas. A investigação de crimes cibernéticos pode ser complexa, exigindo uma combinação de técnicas tradicionais de investigação com métodos especializados, como a análise forense digital (Gomes, 2023).

As autoridades policiais e os órgãos de investigação precisam estar equipados com ferramentas modernas para rastrear atividades criminosas, identificar os perpetradores e coletar evidências que possam ser usadas em processos judiciais (Freitas; Gonçalves e Torres, 2023).

A cooperação internacional é outro aspecto fundamental da repressão aos crimes informáticos. Dada a natureza global da internet, muitos crimes cibernéticos são transnacionais, o que requer colaboração entre diferentes países e organizações internacionais. Tratados e acordos de cooperação, como a Convenção de Budapeste sobre o Cibercrime, facilitam a troca de informações e a coordenação de esforços para combater esses delitos em escala global (Cavalcanti, 2024).

Apesar dos avanços nas ferramentas de prevenção e repressão, diversos desafios persistem no combate aos crimes informáticos. Um dos principais desafios é a rápida evolução das técnicas utilizadas pelos criminosos, que frequentemente estão um passo à frente das medidas de segurança. A anonimidade proporcionada pela internet também dificulta a identificação e a localização dos responsáveis por atividades ilícitas. Além disso, a diversidade de legislações e a falta de harmonização entre os sistemas jurídicos de diferentes países podem complicar a cooperação internacional (Gomes, 2023).

Outro desafio significativo é a proteção da privacidade dos cidadãos. As medidas de segurança e vigilância necessárias para combater os crimes informáticos devem ser equilibradas com a proteção dos direitos fundamentais à privacidade e à liberdade de expressão. Este equilíbrio é delicado e exige uma abordagem cuidadosa e proporcional por parte dos legisladores e das autoridades de segurança (Valente, 2021).

O combate aos crimes informáticos na era digital requer uma abordagem integrada que combine medidas legislativas, tecnológicas e educativas. O Direito Penal desempenha um papel crucial nesse processo, fornecendo a base legal para a tipificação e a punição dessas condutas (Freitas; Gonçalves e Torres, 2023).

No entanto, para que essas ferramentas sejam eficazes, é necessária uma constante atualização das leis e das tecnologias de segurança, bem como uma cooperação internacional robusta. A proteção dos usuários e a garantia de um ambiente digital seguro e confiável são objetivos essenciais que demandam a colaboração de todos os setores da sociedade (Cavalcanti, 2024).

5.2 Fintechs

Fintechs são empresas que combinam tecnologia e inovação para fornecer serviços financeiros de forma ágil, eficiente e acessível. Essas instituições têm transformado o setor financeiro, oferecendo soluções disruptivas e abordagens diferenciadas para atender às necessidades dos consumidores.

Segundo De Paula e Macahyba (2022, on-line), as fintechs são caracterizadas pela adoção de tecnologias avançadas, como inteligência artificial, aprendizado de máquina e blockchain, que possibilitam a automação de processos financeiros e a criação de produtos e serviços inovadores. Essas tecnologias trazem benefícios, como maior conveniência, velocidade nas transações e redução de custos.

> As fintechs são empresas que redesenham a área de serviços financeiros com processos baseados em novas tecnologias, como Inteligência Artificial, Computação em Nuvem e Big Data, para criar um ambiente totalmente digital e automatizado. Isto permite que tais empresas funcionem de maneira remota, sem a necessidade de agências físicas ou mesmo de operadores humanos. Uma das vantagens desta iniciativa é a maior acessibilidade por parte dos

> clientes promovidas pela difusão dos serviços financeiros através de smartphones, permitindo em tese maior agilidade, melhores condições e taxas vinculadas ao serviço. Ao possuírem um custo operacional consideravelmente menor face às instituições tradicionais, elas podem cobrar um valor inferior aos seus clientes pelo serviço financeiro (Ribeiro, 2022, p.34).

No Brasil, as fintechs têm ganhado destaque nos últimos anos, trazendo inovação e transformação para o setor financeiro do país (Santos, 2023). A chegada e evolução dessas empresas foram impulsionadas pelo avanço da tecnologia, o acesso generalizado à internet e a demanda por serviços financeiros mais eficientes e acessíveis.

As fintechs brasileiras oferecem uma ampla gama de serviços, como pagamentos digitais, empréstimos *peer-to-peer*, gestão financeira pessoal, investimentos automatizados e seguros online. Essas soluções disruptivas têm conquistado a atenção dos consumidores, que buscam alternativas ágeis, transparentes e convenientes em comparação aos serviços financeiros tradicionais.

No entanto, a segurança cibernética em fintechs é uma preocupação essencial. Dholakia e Dholakia (2020) destacam que a crescente digitalização e a dependência de sistemas de tecnologia expõem as fintechs a riscos significativos, como a fraude cibernética. Essas ameaças podem comprometer a segurança dos dados dos clientes, a integridade das transações financeiras e a confiança no sistema.

A Autoridade Nacional de Proteção de Dados (ANPD), órgão regulador no Brasil, destaca que as fintechs devem adotar medidas para proteger os dados pessoais dos clientes em conformidade com a Lei Geral de Proteção de Dados (LGPD). O tratamento adequado dessas informações é fundamental para evitar vazamentos, violações de privacidade e uso indevido (Santos, 2023).

A Federação Brasileira de Brancos (FEBRABAN) ressalta que a fraude cibernética é uma das principais preocupações em relação à segurança cibernética em instituições financeiras. Os criminosos utilizam técnicas sofisticadas, como *phishing*, *ransomware* e ataques de engenharia social, para obter acesso não autorizado a contas e informações financeiras. A falta de medidas adequadas de segurança pode expor os clientes a fraudes e prejuízos financeiros.

Para Szor (2005), a fraude cibernética em fintechs é um desafio crítico que precisa ser abordado. Com o rápido crescimento das fintechs e o aumento das transações financeiras online, os fraudadores têm encontrado oportunidades para explorar vulnerabilidades e realizar atividades fraudulentas.

Segundo Christodorescu (2008), a combinação de transações financeiras digitais e o potencial de brechas de segurança tem colocado em risco a integridade das operações e a confiança dos clientes. Os fraudadores utilizam técnicas sofisticadas, como *phishing*, roubo de identidade e ataques de malware, para obter acesso indevido a contas, roubar informações pessoais e realizar transações fraudulentas.

No entanto, é importante estar ciente de que os golpes de *phishing* estão em constante evolução, com os fraudadores se adaptando e utilizando técnicas mais sofisticadas. Portanto, a conscientização e a vigilância contínuas são fundamentais para se proteger contra essa forma de fraude cibernética, conforme esclarece Jakobsson (2007, p.22):

> *Phishing* refere-se à prática fraudulenta de personificar uma entidade legítima, como um banco ou um serviço online, a fim de enganar os usuários para que divulguem suas informações pessoais ou credenciais de login. Esses ataques geralmente envolvem o uso de e-mails ou sites fraudulentos que imitam a aparência de entidades confiáveis, com o objetivo de induzir os usuários a fornecer dados confidenciais que podem ser usados posteriormente para roubo de identidade ou fraude financeira. Como a prevalência de ataques de *phishing* continua a aumentar, é crucial desenvolver contramedidas eficazes para proteger os usuários de serem vítimas dessas fraudes (Jakobsson, 2007, p.22).

As práticas de *phishing* estão se tornando cada vez mais sofisticadas e continuam a ter sucesso devido à combinação de técnicas avançadas de engenharia social e vulnerabilidades de design nas interfaces do usuário, capazes de enganar até mesmo usuários cautelosos a divulgar informações confidenciais.

Mitnick (2002), comenta que essas atividades criminosas têm impactos significativos tanto para as fintechs quanto para os usuários. Além de causar danos financeiros, as fraudes cibernéticas podem prejudicar a reputação das empresas e abalar a confiança dos clientes no uso de serviços financeiros online.

Hadnagy (2016), diante desse cenário, é crucial que as fintechs adotem medidas robustas de segurança cibernética para proteger seus sistemas e os dados dos clientes. Isso envolve a implementação de tecnologias de criptografia, autenticação em duas etapas, monitoramento contínuo de atividades suspeitas e educação dos usuários sobre práticas seguras. Além disso, é importante que exista uma legislação adequada e eficaz para combater a fraude cibernética em fintechs. As leis devem abranger punições adequadas para os criminosos e fornecer orientações claras sobre responsabilidades e requisitos de segurança cibernética para as empresas do setor.

Pontel (2014), esclarece que a colaboração entre as fintechs, órgãos reguladores, autoridades policiais e especialistas em segurança cibernética é essencial para enfrentar o desafio da fraude cibernética. Compartilhar informações sobre ameaças, boas práticas e soluções de segurança pode ajudar a fortalecer a resiliência do setor financeiro digital. Em resumo, a fraude cibernética representa uma ameaça significativa para as fintechs. É fundamental que essas empresas invistam em segurança cibernética robusta, estejam em conformidade com a legislação e trabalhem em conjunto com as partes interessadas para combater a fraude, proteger os clientes e preservar a confiança no ambiente digital das fintechs.

6 CONCLUSÃO

A presente monografia revelou que a evolução tecnológica e a expansão da internet, embora tenham proporcionado inúmeros benefícios para a sociedade, também intensificaram a vulnerabilidade dos consumidores a diversos tipos de crimes informáticos. A análise detalhada da conexão digital e dos desafios impostos pelos crimes cibernéticos mostrou que a expertise e a proficiência tecnológica dos criminosos criam uma disparidade significativa em relação ao consumidor, que frequentemente se encontra despreparado para enfrentar tais ameaças.

A pesquisa evidenciou que a legislação, tanto nacional quanto internacional, tem avançado no sentido de reprimir os crimes informáticos. A implementação de leis específicas, como a Lei Carolina Dieckmann e a Lei nº 13.709 de 14 de agosto de 2018, representa passos importantes na proteção dos usuários. Contudo, a rápida

evolução das técnicas utilizadas pelos criminosos exige uma constante atualização e adaptação das normas jurídicas, bem como o desenvolvimento de novas estratégias de prevenção e repressão.

A tipologia dos crimes informáticos, abrangendo desde golpes nas relações de consumo até crimes mais graves como a pedofilia online e o cyberbullying, demonstra a complexidade e a variedade das ameaças presentes no ambiente digital. Este estudo destacou a importância de uma abordagem multidisciplinar para enfrentar esses desafios, combinando esforços legislativos, tecnológicos e educacionais. A educação digital emerge como uma ferramenta crucial para capacitar os consumidores a identificar e evitar possíveis riscos, fortalecendo assim a sua segurança online.

Além disso, a pesquisa enfatizou a necessidade de uma colaboração internacional mais estreita, dado que a natureza global da internet permite que os criminosos operem além das fronteiras nacionais. A cooperação entre diferentes países e organizações internacionais é fundamental para a criação de um ambiente digital mais seguro e resiliente, onde as práticas criminosas possam ser mais eficientemente monitoradas e combatidas.

Por fim, conclui-se que, embora os desafios impostos pelos crimes informáticos sejam numerosos e complexos, a combinação de legislações atualizadas, tecnologias avançadas e uma educação digital robusta pode proporcionar um caminho eficaz para a proteção dos consumidores. A conscientização sobre as vulnerabilidades e a adoção de medidas preventivas e repressivas adequadas são essenciais para garantir a segurança e a confiança no ambiente digital, permitindo que os benefícios da internet possam ser plenamente usufruídos pela sociedade.

REFERÊNCIAS

ALMEIDA, Jessica de Jesus *et al*. Crimes cibernéticos. **Caderno de Graduação-Ciências Humanas e Sociais (UNIT),** Sergipe, v. 2, n. 3, p. 215-236, 2015.

ALICERAL, Denise Ribeiro. **O direito de arrependimento no CDC**: a vulnerabilidade do consumidor e a necessidade de ampliação da abrangência do artigo 49. 2014. 66f. Monografia (Bacharelado em Ciências Jurídicas e Sociais) - Centro Universitário de Brasília – UniCEUB, Salvador, 20214.

BARBOSA, Mateus Israel Alves Crivinel. **Crimes virtuais**: A evolução dos crimes cibernéticos e os desafios no combate. 2020. 24f. Artigo Científico (Graduação em Direito) - Pontifícia Universidade Católica de Goiás, Goiânia.

BARROS, Rebeca Buarque de Araujo. **Da responsabilidade civil decorrente das ofensas aos direitos de personalidade no âmbito virtual**. 2021. 95f. TCC (Bacharelado em Direito) - Faculdade de Direito de Alagoas (FDA/UFAL), Maceió, 2021. Disponível em: <https://www.repositorio.ufal.br/handle/123456789/10110>. Acesso em: 11 de julho de 2024.

BATISTA, Lorena Prado. **Crimes cibernéticos uma análise sobre como a tecnologia está a serviço da criminalidade no brasil.** 2022. 20f. Artigo Científico (Graduação em Direito) — Pontifícia Universidade Católica de Goiás, Goiânia, 2022. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/4706/1/Trabalho%20LORENA%20Prado.pdf>. Acesso em: 11 de julho de 2024.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais – **A Função e os Limites do Consentimento.** São Paulo: Editora Forense, 2018.

BIONI, Bruno Ricardo. GOMES, Maria Cecilia Oliveira; MONTEIRO, Renato Leite. GDPR matchup: Brazil's General Data Protection Law. Available at: [https://iapp.org/news/a/gdpr-matchup-brazilsgeneral-data-protection-law/]. Cf. also MENDES, Laura Schertel and DONEDA, Danilo. Initial reflections on the new General Data Protection Law. In: **Revista de Direito do Consumidor**, v. 120, Nov.-Dec. 2018, p. 469-483.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**. Parte Geral 1. 13th ed. SãoPaulo: Saraiva, 2008.

BORTOT, Jessica Fagundes. Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. **Virtuajus**, v. 2, n. 2, p. 338-362, 2017. Disponível em: <http://periodicos.pucminas.br/index.php/virtuajus/article/view/15745>. Acesso em: 11 de julho de 2024.

BORGES, Liliane de Moura. **Enfim, chegou a tão esperada atualização do Código de Defesa do Consumidor**. FASEC – Faculdade Serra do Carmo, 2021. Disponível em: <https://serradocarmo.edu.br/4709-2/>. Acesso em: 05 jun. 2024.

BRASIL. Constitution (1988). Constitution of the Federative Republic of Brazil. Brasília, DF: Senado Federal, 1988. Available at: http://goo.gl/Y9JnrU **Accessed on June** 3, 2024.

BRASIL. Law No. 12,965, of April 23, 2014. **Establishes principles, guarantees, rights, and duties for the use of the Internet in Brazil.** Brasília, DF, Apr 23, 2014. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Accessed on April 5, 2024.

BRASIL. Law No. 12,737, of November 30, 2012. **Provides for the criminal typification of computer crimes; amends Decree-Law** No. 2,848, of December 7, 1940 - Penal Code; and other provisions. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Accessed on May 6, 2024.

BRASIL. Law No. 13,709/2018, of August 14, 2018. **General Data Protection Law (LGPD).** [S. l.], April 19. 2024

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 11 de julho de 2024.

BRASIL. **Lei n°12.737 de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 11 de julho de 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da República Federativa do Brasil, Brasília, DF, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 11 de julho de 2024.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão. **Crimes cibernéticos**. Brasília: MPF, 2018. Disponível em: <https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos>. Acesso em: 11 de julho de 2024.

CARDOSO, **A vulnerabilidade do direito à informação nas relações de consumo pelos meios digitais**: uma análise sobre a necessidade de consentimento e controle do consumidor sobre o destino de seus dados pessoais. 2022. 91f. TCC (Bacharelado em Direito) - Universidade Federal de Santa Catarina, Florianópolis, 2022.

CANTO, Rodrigo Eidelvein do. **A vulnerabilidade dos consumidores no comércio eletrônico e a reconstrução da confiança na atualização do código de defesa do consumidor**. 2014. 224f. Dissertação (Mestrado em Direito Privado) - Curso de Direito, Faculdade de Ciências Jurídicas e Sociais, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014.

CAVALCANTI, Chris Marçal. **Crimes cybernéticos:** liberdade de expressão. 2024.

CARVALHO, Patrícia Heloisa de. O "Marco Civil Da Internet": Uma Análise sobre A constitucionalidade do artigo 19. **Revista da Faculdade de Direito do Sul de Minas**, v. 33, n. 2, 2017.

CHAGAS, Jefison de Andrade das. **As mudanças trazidas pela lei geral de proteção de dados e suas implicações na proteção de dados pessoais dos consumidores pelas empresas privadas**. 2023. 121f. Dissertação (Mestrado em Direito) – Universidade Federal de Sergipe – UFS, São Cristóvão, 2023. Disponível em: <https://ri.ufs.br/bitstream/riufs/17310/2/JEFISON_ANDRADE_CHAGAS.pdf>. Acesso em: 11 de julho de 2024.

CHRISTODORESCU, M., JHA, S., & SESHIA, S. A. (2008). ***Malware* detection**. IEEE Computer, 41(4), 48-55.

CIDRÃO, T. V.; MUNIZ, A. W.; ALVES, A. A. The timely and necessary implementation of International Law in the cyberspace: from the Budapest Convention to Brazilian legislation. **Brazilian Journal of International Relations**, Marília, SP, v. 7, n. 1, p. 66–82, 2018. DOI: 10.36311/2237-7743.2018.v7n1.01.p66. Available at: https://revistas.marilia.unesp.br/index.php/bjir/article/view/7069. Accessed on June 2, 2024.

COELHO, Ivana Pereira; BRANCO, Sérgio. Humor e Ódio na Internet. **Cadernos Adenauer XV**, Rio de Janeiro, 2016. Disponível em: <https://www.academia.edu/30091847/Humor_e_%C3%B3dio_na_internet>. Acesso em: 11 de julho de 2024.

COSTA, Vair. **Os crimes cibernéticos, a responsabilidade civil do provedor e a classificação dos seus serviços**. 2019. 82f. Monografia (Bacharelado em Direito) - Faculdades Integradas de Caratinga (DOCTUM), Caratinga, MG, 2019. Disponível em: <http://dspace.doctum.edu.br:8080/bitstream/123456789/1979/1/TCC%202019%20..pdf>. Acesso em: 11 de julho de 2024.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.90.

CHRISTODORESCU, M., JHA, S., & SESHIA, S. A. (2008). ***Malware* detection**. IEEE Computer, 41(4), 48-55.

CRIMES VIRTUAIS: conceito e seus tipos. **Available at jus Brasil:** https://carmo311.jusbrasil.com.br/artigos/307607071/crimes-virtuais-conceito-e-seus-tipos Accessed on June 2, 2024, at 12:11.

CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. **Revista Científica Eletrônica do Curso de Direito**, v.13, p.1-18, 2018. Disponível em: <http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf>. Acesso em: 11 de julho de 2024.

CZELUSNIAK, Vivian Amarro. O consumidor pessoa jurídica sob uma análise jurisprudencial. **Revista Direito e Justiça: Reflexões Sociojurídicas**, Santo Ângelo, v. 19, n. 33, p. 161-182. 2019.

DURAN, Laís Baptista Toledo; BARBOSA, Laryssa Vicente Kretchetoff. LEI CAROLINA DIECKMANN: Atualização jurídico-normativa brasileira. **ETIC - Encontro de Iniciação Científica**, v. 11, n. 11, 2015.

DHAMIJA, R., TYGAR, J. D., & HEARST, M. (2006). **Why phishing works. In Proceedings of the** SIGCHI conference on Human Factors in Computing Systems (pp. 581-590).

DHOLAKIA, U. M., & DHOLAKIA, R. R. (2020). **Fintech Frauds: Taxonomy, Ethical and Legal Challenges. Journal of Business Research**, 119, 550-558.

FERREIRA, Renan Azevedo Leonessa. **Crimes informáticos: estudos a partir da vítima**. Editora Dialética, 2023.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital.** São Paulo: Saraiva Educação SA, 2017.

FONSECA, Gabriel Alves. A boa-fé objetiva e a assimetria informacional como legitimadoras do dever de informar nas relações de consumo: O exemplo do consentimento informado entre médico e paciente. **Revista dos Estudantes de Direito da Universidade de Brasília**, v. 1, n. 21, p. 179-207, 2022.

FUMAGALLI, L., MAGGI, F., CAVALLARO, L., & ZANERO, S. (2016). **Investigating identity theft in the wild**. IEEE Security & Privacy, 14(3), 46-54.

FREITAS, Camila Cristina Gonzaga; GONÇALVES, Jonas Rodrigo; TORRES, Mateus Guimarães. A evolução do direito penal brasileiro relacionado aos crimes cibernéticos. **Revista JRG de Estudos Acadêmicos**, v. 6, n. 12, p. 296-311, 2023.

GARCIA, Plinio da Silva. **Influência do ambiente organizacional na motivação para prática de crimes cibernéticos**. 2016. 114f. Dissertação (Mestrado em Administração) - Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre. Disponível em: <https://tede2.pucrs.br/tede2/handle/tede/6946>. Acesso em: 11 de julho de 2024.

GOMES, LUANA. **Crimes Virtuais: O Limite Da Liberdade De Expressão**. Instituto Metropolitano de Educação e Cultura LTDA. - Faculdade Metropolitana Anápolis. 2023.Disponível em: https://repositorio.faculdadefama.edu.br/xmlui/handle/123456789/205 acesso em: 17 de julho de 2024.

GRECO, Rogério. **Curso de Direito Penal**. Parte Geral. 13th Ed. Rio de Janeiro: Editora Impetus.

HADNAGY, C. (2011). **Social Engineering**: The Art of Human Hacking. Wiley Publishing.

HORBYLON, Isabella. **Os crimes cibernéticos perante o ordenamento jurídico brasileiro**: Os haters atrás das telas. 2022. 27f. Artigo Científico (Bacharelado em Direito) – Pontifícia Universidade Católica de Goiás, Goiânia, 2022. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/4578/1/Artigo%20Cienti%CC%81fico-%20%20-ISADORA%20HORBYLON.pdf>. Acesso em: 11 de julho de 2024.

JAKOBSSON, M., & MYERS, S. A. (2007). **Phishing and countermeasures: understanding the increasing problem of electronic identity theft**. Wiley Publishing.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

LEHFELD, Lucas de Souza *et al*. A (hiper) vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. **Revista Eletrônica Pesquiseduca**, v. 13, n. 29, p. 236-255, 2021. Disponível em: <https://periodicos.unisantos.br/pesquiseduca/article/view/1029>. Acesso em: 11 de julho de 2024.

LIMA, Cláudio Vieira Guimarães. **Crimes cibernéticos**: O lado obscuro da rede. 2021. 27f. Monografia Jurídica (Bacharelado em Direito) - Pontifícia Universidade Católica de Goiás, Goiânia, 2021. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/2419>. Acesso em: 11 de julho de 2024.

MATSUYAMA, Keniche Guimarães; LIMA, JAA. **Cybercrimes: atypicality of crimes**. 2017.

MARRA, F. B. (2019). **Challenges of Law in the Internet Age:** a brief analysis of cybercrimes. Journal of Law and Sustainable Development, 7(2), 145–167. https://doi.org/10.37497/sdgs.v7i2.51

MARRA, Fabiane Barbosa. Desafios do direito na era da internet: uma breve análise sobre os crimes cibernéticos. **Journalof Law andSustainableDevelopment**, v. 7, n. 2, p. 145-167, 2019.

MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito**, v. 106, p. 01-17, 2017. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RDCons_n.106.02.PDF>. Acesso em: 11 de julho de 2024.

MESQUITA, Nathalia Rayane Alves Mesquita. **A Lei Geral de Proteção de Dados (LEI 13.709/18): Desafios da proteção de dados pessoais nos meios digitais**. 2021. Artigo Científico (Graduação em Direito) — Pontifícia Universidade Católica de Goiás, Goiânia, 2021.

MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito**, v. 106, p. 01-17, 2017. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RDCons_n.106.02.PDF>. Acesso em: 11 de julho de 2024.

MIRAGEM, Bruno. **Direito civil**: direito das obrigações. 2. ed. São Paulo: Saraiva, 2018.

MIRAGEM, Bruno. Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor. **Revista de Direito do Consumidor**, p. 17-62, 2020.

MITNICK, K. D., & SIMON, W. L. (2002). **The Art of Deception:** Controlling the Human Element of Security. John Wiley & Sons.

MOURA, Grégore Moreira de; **Curso de Direito Penal Informático**- 1st Ed- Belo Horizonte: D'Plácido, 2021.

MODENESI, Pedro de Melo. **A proteção do ciberconsumidor e o princípio da boa-fé objetiva**. 2010. 160f. Dissertação (Mestrado em Direito Civil Constitucional; Direito da Cidade; Direito Internacional e Integração Econômica e Direito Privado) - Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2010. Disponível em: <https://www.bdtd.uerj.br:8443/handle/1/9407>. Acesso em: 11 de julho de 2024.

NASCIMENTO, Carlo Bruno Lopes do. A problemática da informação imperfeita nas relações de consumo e a necessidade de proteção do vulnerável. **Revista do Instituto do Direito Brasileiro**, ano 1, n. 2, p. 381-408, 2015.

ORRIGO, Gabriel Marcos Archanjo; FILGUEIRA, Matheus Henrique Balego. Crimes Cibernéticos: Uma abordagem jurídica sobre os crimes realizados no âmbito virtual. **ETIC-Encontro de Iniciação Científica**, v. 11, n. 11, 2015.

PACÍFICO, Marsiel; GOMES, Luiz Roberto. Deep Web: o que podemos compreender olhando para o invisível? **Tríade: Comunicação, Cultura e Mídia**, v. 9, n. 22, p. 181-203, 2021.

PINTO, Vinicius de Assis; DINIZ, Carine Silva. Vulnerabilidade do consumidor no ciberespaço e a lei geral de proteção de dados. **Direito Izabela Hendrix**, v. 29, n. 29, 2022.

PINHEIRO, Patricia Peck. **Direito digital**. 6. ed. São Paulo: Saraiva, 2016.

PONTELL, H. N., GEIS, G., & BROWN, R. (2014). **The Professional Con Artist and Occupational Fraud.** In Occupational and Organizational Crime (pp. 42-64). Palgrave Macmillan.

REZENDE, Vinícius Biagioni; DE SOUZA PAULA, Daniel Henrique. O comércio eletrônico e a defesa do consumidor nas relações de consumo. **Brazilian Journal of Development**, v. 7, n. 5, p. 47882-47901, 2021.

RIBEIRO, Alexandre Ogêda. **Aspectos concorrenciais das *fintechs* na indústria financeira nacional.** 2022.

RODRIGUES, Ana Luiza Garcêz. **Lei Geral de Proteção de Dados**: O importante papel da autoridade nacional de proteção de dados e a busca pela defesa do consumidor e titular de dados. 2021. 44f. Monografia (Bacharelado em Direito) - Pontifícia Universidade Católica de Goiás, Goiânia, 2021. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/2561. Acesso em: 11 de julho de 2024.

RODRIGUES, Sandrielem da Silva; GALDI, Fernando Caio. Relações com investidores e assimetria informacional. **Revista Contabilidade & Finanças**, v. 28, n.74, p. 297-312, 2017.

SANTOS, Junior. **Como as Fintechs estão transformando o sistema financeiro brasileiro!**

Disponível em: https://pt.linkedin.com/pulse/como-*fintechs*-est%C3%A3o-transformando-o-sistema-junior-santos acesso em 11 de jul 2024.

SZOR, P. (2005). **The Art of Computer Virus Research and Defense**. Pearson Education.2005.

SILVA, Carlos Mendes Monteiro da; MARTINS, Luana Maria; MARQUES FILHO, Elvis Gomes. O consumidor digital pode ser considerado um sujeito hipervulnerável? **Ciências Sociais Aplicadas em Revista**, v. 22, n. 42, p. 17-31, 2022.

SILVA, Debora Cristina da. **Cibercriminalidade e a (in) suficiência legislativa pátria para a repressão dos crimes cometidos por meio da internet**. 2020. 106f. TCC (Bacharelado em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2020. Disponível em:

<https://repositorio.ufsc.br/bitstream/handle/123456789/218882/TCC%20-%20FINAL.pdf?sequence=1&isAllowed=y>. Acesso em: 11 de julho de 2024.

SILVA, Jefferson Ximenes da *et al*. Marketing digital nas redes sociais. **Observatorio de la Economía Latinoamericana**, n. 243, 2018. Disponível em: <https://www.eumed.net/rev/oel/2018/05/marketing-redes-sociais.zip>. Acesso em: 11 de julho de 2024.

SILVA, Ingryd Martins. **A infiltração policial como técnica especial de investigação no ambiente cibernético**. 2017. 83f. TCC (Bacharelado em Direito) - Instituto de Ciências da Sociedade de Macaé da Universidade Federal Fluminense, Macaé, RJ, 2017. Disponível em: <https://app.uff.br/riuff/handle/1/4955>. Acesso em: 11 de julho de 2024.

SOUZA, Allan Rocha de. Cultura, Revolução tecnológica e os direitos autorais. In: MARTINS, Guilherme Magalhães Martins; LONGHI, João Victor Rozatti. **Direito digital: direito privado e internet**. 3. ed. Indaiatuba, São Paulo: Editora Foco, 2020.

TEIXEIRA, Felipe Silva; CHAVES, Fábio Barbosa. **Os crimes de fraude e estelionato cibernéticos e a proteção ao consumidor no e-commerce**. Jus.com.br, 2019. Disponível em: <https://jus.com.br/artigos/73480/os-crimes-de-fraude-e-estelionato-ciberneticos-e-a-protecao-ao-consumidor-no-e-commerce>. Acesso em: 11 de julho de 2024.

TEIXEIRA, Tarcisio. **Comercio Eletrônico:** Conforme o Marco Civil Da Internet e a regulamentação do e-commerce no Brasil. São Paulo: Saraiva Educação SA, 2015.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, v. 30, n.86, p. 269-285, 2016.

TORRES JÚNIOR, Paulo Fernando Moreira. **O direito à privacidade e à intimidade na internet**. 2015. 25f. TCC (Bacharelado em Direito) – Universidade Tiradentes (UNIT), Aracaju, 2015.

VALENTE, VICTOR AUGUSTO ESTEVAM. Lacunas jurídicas e crimes informáticos: comentários sobre o tratamento acerca do crime de pornografia infantil na internet. **Cadernos de Dereito Actual**, n. 15, p. 95-129, 2021.

VIEIRA, Jerônimo Araújo de Deus et al. Aplicação de cenários prospectivos ao planejamento de tecnologia da informação e comunicação: Estudo de caso da PMDF. **Revista Ciência & Polícia**, v. 8, n. 2, p. 73-110, 2022.