UNIVERSIDADE PAULISTA

GUILHERME MARCELINO GONÇALVES

CRIMINALIDADE NA INTERNET
CRIMES VIRTUAIS, CRIMES CIBERNÉTICOS

SANTOS
2025

GUILHERME MARCELINO GONÇALVES

CRIMINALIDADE NA INTERNET
CRIMES VIRTUAIS, CRIMES CIBERNÉTICOS

Trabalho de conclusão de curso para obtenção do título de graduação em Direito apresentado à Universidade Paulista – UNIP.
Orientadora: Profª Ana Paula Martin Martins

SANTOS
2025

GUILHERME MARCELINO GONÇALVES

CRIMINALIDADE NA INTERNET
CRIMES VIRTUAIS, CRIMES CIBERNÉTICOS

Trabalho de conclusão de curso para obtenção do título de graduação em Direito apresentado à Universidade Paulista – UNIP.
Orientadora: Profª Ana Paula Martin Martins

Aprovado(a) em: _____/_____/_____

BANCA EXAMINADORA

Prof. ou Profa. Dr(a)./Me(a). xxxxxxxxxxx
Universidade Paulista - UNIP

Prof. ou Profa. Dr(a)./ Me(a). xxxxxxxxxxx
Universidade Paulista - UNIP

Prof. ou Profa. Dr(a)./ Me(a). xxxxxxxxxxx
Universidade Paulista - UNIP

AGRADECIMENTOS

Gostaria de expressar minha sincera gratidão a todas as pessoas que, de alguma forma, contribuíram para a realização deste trabalho.

Primeiramente, agradeço *à* minha orientador*a*, *Ana Paula Martin Martins*, pela orientação, paciência e dedicação, que foram fundamentais para o desenvolvimento deste estudo. Aos professores durante toda a jornada que com sua expertise e formação acadêmica me ajudaram a compreender as complexidades do tema e a aprimorar a análise da criminalidade no contexto virtual.

Agradeço também aos meus colegas e amigos, que, com suas conversas e reflexões, contribuíram para enriquecer a abordagem teórica e prática deste trabalho. Suas opiniões e sugestões foram sempre valiosas.

Por fim, agradeço a todas as fontes e pesquisas que, de alguma forma, ajudaram a formar a base deste estudo. O trabalho de tantos pesquisadores, estudiosos e especialistas na área da criminalidade cibernética foi uma fonte constante de aprendizado e inspiração.

A todos, o meu mais profundo agradecimento.

DEDICATÓRIA

Dedico este projeto com muito carinho e gratidão a algumas pessoas importantes que estiveram comigo em cada etapa deste percurso.

À minha mãe, que foi e continua a ser minha principal fonte de apoio e inspiração da qual me inspirou a seguir o mesmo caminho em que ela seguiu. O seu amor incondicional, dedicação e ensinamentos formam a base firme sobre a qual construí meu caminho. Não existem palavras que consigam expressar o quanto sou grato por tudo que fez por mim, pelos sacrifícios e por ter acreditado em mim, mesmo quando eu mesmo tinha dúvidas.

À minha namorada Larissa, que, com muita paciência, compreensão e afeto, esteve ao meu lado nos momentos difíceis, me motivando a continuar e a não desistir. Sua presença na minha vida é um lembrete constante de que o amor e o apoio mútuo tornam mais fáceis todos os obstáculos.

À minha família, que sempre me ofereceu um lar acolhedor e cheio de amor, com cada um de vocês me ensinando a importância da união, da persistência e do compromisso. Sem a ajuda de todos, eu não estaria aqui.

Este projeto é, sem dúvida, um reflexo de tudo que recebi de vocês. Agradeço por estarem ao meu lado em todos os momentos deste trajeto.

“Posso não concordar com o que tu dizes, mas lutarei, para que o possas dizer em liberdade”

(VOLTAIRE)

RESUMO

O presente trabalho busca analisar o impacto do avanço tecnológico na sociedade, destacando os crimes virtuais e a forma como a tecnologia facilita o anonimato dos infratores. O estudo investiga, através de pesquisas, quais são as vítimas mais afetadas e vulneráveis em um contexto onde a internet se tornou uma necessidade do dia a dia dos indivíduos. A pesquisa aborda a prevalência dos crimes virtuais, detalhando os tipos mais comuns e como eles ocorrem, além de apresentar as leis e as medidas da legislação penal brasileira que são utilizadas pelas autoridades para combater a criminalidade na Internet. O trabalho é fundamentado em artigos acadêmicos e análises de uma pesquisa quantitativa realizada pela universidade FGV, que permitiram identificar não apenas a faixa etária mais afetada, mas também os meios mais frequentemente utilizados para a prática dos crimes virtuais. Dessa forma, o estudo visa não só esclarecer os tipos de crimes digitais e suas implicações, mas também discutir o papel da sociedade na prevenção e combate, alertando sobre os riscos e a exposição excessiva na internet. Através dessas abordagens, o trabalho busca promover uma conscientização mais profunda e informar sobre medidas de proteção, reforçando a importância da educação digital e da responsabilidade coletiva para minimizar os impactos negativos da tecnologia.

Palavras-chave: crimes virtuais; vítimas; crimes digitais; Internet.

ABSTRACT

This work seeks to analyze the impact of technological advances on society, highlighting virtual crimes and the way in which technology facilitates the anonymity of offenders. The study investigates, through research, which victims are most affected and vulnerable in a context where the internet has become a necessity in individuals' daily lives. The research addresses the prevalence of virtual crimes, detailing the most common types and how they occur, in addition to presenting the laws and measures of Brazilian criminal legislation that are used by authorities to combat crime on the Internet. The work is based on academic articles and analyzes of quantitative research carried out by the FGV university, which made it possible to identify not only the most affected age group, but also the means most frequently used to commit virtual crimes. Therefore, the study aims not only to clarify the types of digital crimes and their implications, but also to discuss the role of society in preventing and combating them, warning about the risks and excessive exposure on the internet. Through these approaches, the work seeks to promote deeper awareness and inform about protective measures, reinforcing the importance of digital education and collective responsibility to minimize the negative impacts of technology.

Keywords: virtual crimes; victims; digital crimes; Internet.

SUMÁRIO

INTRODUÇÃO

A delinquência online, conhecida como crimes virtuais e cibernéticos, tornou-se uma das principais inquietações nas sociedades modernas, especialmente com o aumento do uso de tecnologias digitais e a transformação do espaço físico em digital. Esse fenômeno abrange uma vasta gama de ações ilegais realizadas por meio de redes de computadores, incluindo fraudes financeiras, roubo de informações pessoais, invasão de sistemas, ataques cibernéticos, calúnias na internet, assédio online, entre outros. As fronteiras do crime cibernético muitas vezes são complicadas de definir, pois, ao contrário dos delitos tradicionais, as infrações virtuais podem ultrapassar divisões geográficas e jurídicas, tornando a investigação e a punição mais complicadas.

Com o aumento da conectividade e a digitalização de serviços e processos, a internet se tornou um ambiente amplo e atrativo para atividades criminosas, gerando impactos significativos na segurança pública e na privacidade dos cidadãos. Os cibercriminosos se valem de métodos avançados, como engenharia social, phishing, malware, ransomware e outras ferramentas para explorar as fraquezas de sistemas, redes e equipamentos. Além disso, crimes como o tráfico de informações sigilosas e o uso indevido de dados pessoais são preocupações constantes, especialmente com o crescimento das transações comerciais e interações sociais online.

A característica global da internet complica a aplicação das legislações, uma vez que os infratores podem operar de qualquer parte do planeta, dificultando ainda mais o rastreamento e a responsabilização. A falta de uma legislação uniforme em muitos países também contribui para a inconsistência nas respostas legais aos crimes cibernéticos. Isso exige uma cooperação internacional cada vez mais robusta para o enfrentamento dessas violações, além da criação de estruturas legais e tecnológicas que acompanhem a evolução das ameaças digitais.

Nesse cenário, a criminalidade online envolve não apenas a atuação dos infratores, mas também suscita questões sobre a responsabilidade das

empresas de tecnologia, a proteção dos dados dos usuários e a educação digital. A sociedade precisa se preparar adequadamente para enfrentar os riscos do ambiente virtual, por meio de uma combinação de legislações eficientes, políticas de segurança da informação e conscientização pública. O desafio é considerável, mas a colaboração crescente entre governos, empresas e cidadãos pode levar a um ambiente digital mais seguro e confiável para todos.

1. **A CRIMINALIDADE NO CONTEXTO TECNOLÓGICO**

O advento das tecnologias da informação e comunicação transformou profundamente a sociedade contemporânea, afetando diretamente a maneira como os indivíduos se relacionam, trabalham, consomem e, infelizmente, também como cometem crimes. A criminalidade, antes restrita ao espaço físico, encontra no ambiente digital um novo território fértil para sua expansão, caracterizando o que se convencionou chamar de crimes cibernéticos ou crimes digitais.

> "Os crimes realizados no meio virtual são denominados de crimes virtuais, digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, fraude informática, delitos cibernéticos, crimes transnacionais, dentre outras nomenclaturas." (MAUES; DUARTE; CARDOSO, 2018, p. 170).

Pode-se dizer que a Internet deixou de ser um facilitador da comunicação e passou a ser uma ferramenta indispensável para o cotidiano do ser humano, acarretando a praticidade, mas também com muitos pontos negativos a serem mencionados.
Com o avanço da tecnologia e a rápida disseminação de informações, tornou-se mais difícil controlar as atividades dos usuários no ambiente digital, o que faz com que individuo naveguem sem que suas identidades verdadeiras sejam expostas.

> "Na atualidade, o papel da *Internet* estende-se para além de um simples meio de comunicação,porquanto passou a fazer parte da própria vida em sociedade como facilitador e mantedor de relações humanas." (PIMENTEL; CARDOSO, 2015, p. 48)

Desta forma, é possível concluir que a sociedade está em constante mutação em vários aspectos, dentre eles, a evolução digital, onde ganhou espaço para a praticidade na execução de crimes virtuais, o que acarreta a dificuldade para a sanção institucionalizada para com os criminosos do âmbito cibernético.

> "Com o advento da pandemia, houve um aumento significativo no uso de dispositivos eletrônicos conectados à internet, o que contribuiu para o crescimento desses crimes. A simplicidade desses crimes levou a uma migração do crime tradicional para o mundo virtual, devido à menor exposição do criminoso" (DORIGON; SOARES, 2018).

Os crimes cometidos no ambiente digital cresceram significativamente com o modo que a tecnologia foi se desenvolvendo e ganhando espaço na sociedade, o que apresenta um grande desafio para a correta identificação dos responsáveis e a consequente aplicação das penalidades legais. Assim, é importante destacar que a complexidade das tecnologias utilizadas para mascarar identidades, como o uso de redes privadas virtuais (VPNs) e criptografia, corroboram para dificultar o rastreamento dos infratores. Além disso, a legislação em muitas regiões ainda está em processo de adaptação para acompanhar a rápida evolução do mundo digital, o que torna ainda mais difícil combater e punir crimes cibernéticos de forma eficaz. Portanto, a colaboração entre especialistas em segurança cibernética, autoridades legais e organizações internacionais é crucial para o desenvolvimento de estratégias que permitam uma resposta mais ágil e precisa aos delitos virtuais. Assim sendo, é preciso destacar que:

> "O acesso às novas tecnologias em um mundo cada vez mais conectado têm garantido diversos avanços nas relações sociais e econômicas. Entretanto, toda essa tecnologia também pode ser utilizada para a prática de crimes. Os crimes cibernéticos são uma realidade, várias espécies de crimes se originaram e outros já conhecidos ganharam uma nova roupagem diante do avanço tecnológico" (ARAÚJO, 2018, p. 90)

Estudos destacam que quanto mais se utiliza a Internet desde uma ferramenta para comunicação até para maiores ações o risco de crimes cibernéticos aumentam, assim potencializando o surgimento de novos crimes através da Internet.

Embora hoje não há um termo ou nomenclatura a ser utilizada quando se trata de crimes pela Internet, o Brasil conta com o IBDE (Instituto Brasileiro de Direito Econômico) que concentra e tem papel de mediador para crimes virtuais, eletrônico, crime de informática, dentre outros, no entanto, se trata de uma conduta que fere um bem jurídico na qual seja praticada através de meios de informática (celular, computador, notebook, tablets...).

1.1. QUEM COMETE ESSES CRIMES?

No âmbito jurídico, o indivíduo que realiza uma conduta criminosa é chamado de autor, agente ou sujeito ativo do crime. Essa definição se aplica tanto a infrações cometidas de forma tradicional quanto àquelas realizadas no ambiente digital. A responsabilidade penal recai sobre esse agente, seja ele praticante de crimes culposos, ou seja, quando há negligência, imprudência ou imperícia, ou dolosos, nos quais há a clara intenção de lesar a vítima ou burlar sistemas legais.

No contexto da criminalidade na internet, a identificação do sujeito ativo se torna um desafio técnico e legal considerável. Frequentemente, esses indivíduos são chamados popularmente de “hackers”, uma denominação que, embora amplamente utilizada pela mídia, é imprecisa do ponto de vista técnico e ético. Tradicionalmente, o termo hacker designava pessoas com alto conhecimento técnico em computação, capazes de acessar sistemas com fins exploratórios ou de aprendizado, muitas vezes sem a intenção de causar danos. Contudo, ao longo dos anos, essa concepção foi distorcida e passou a ser associada automaticamente a cibercriminosos.

> Apesar do termo *hacker* sempre aparecer associado a roubo de dados e invasão de sistemas, no entendimento de especialistas em computação, os verdadeiros criminosos são designados como *crackers.* A palavra deriva do verbo em inglês “to crack”, que significa quebrar. Entre as ações, estão a prática de quebra de sistemas de segurança, códigos de criptografia e senhas de acesso a redes, de forma ilegal e com a intenção de invadir e sabotar para fins criminosos. O termo *hacker,* por sua vez, serve para designar um programador com amplo conhecimento sobre sistemas, mas sem a intenção de causar danos. Inclusive, a habilidade para lidar com sistemas e programações, muitas vezes, é utilizada pela própria polícia em investigações ou até mesmo no desenvolvimento de *softwares* com o intuito de limar brechas de segurança, criar novas funcionalidades ou adaptar as antigas. (CASSANTI, Moisés, 2014, p. 2).

Com o amadurecimento das discussões em torno do cibercrime, novas classificações surgiram para diferenciar os tipos de ações e os perfis dos agentes digitais. Um exemplo é o termo "cracker", mais adequadamente utilizado para se referir àqueles que, de maneira maliciosa, invadem sistemas, burlam mecanismos de segurança, roubam dados sensíveis e causam prejuízos, tanto financeiros quanto morais, a indivíduos, empresas ou

instituições públicas. O cracker age deliberadamente, com objetivos que vão desde o ganho financeiro ilícito até o ciberterrorismo ou a vingança pessoal.

Além dos crackers, há ainda outros perfis de agentes virtuais que contribuem para a criminalidade online, como os scammers (especialistas em aplicar golpes virtuais), os phishers (que utilizam técnicas de engenharia social para obter dados confidenciais das vítimas), os carders (voltados para a clonagem e comercialização de cartões de crédito), os spammers (que disseminam conteúdo não solicitados, muitas vezes maliciosos), e até os chamados script kiddies, indivíduos com pouco conhecimento técnico que usam ferramentas prontas para realizar ataques simples, motivados por diversão ou desejo de notoriedade.

É importante destacar que, na era digital, a criminalidade na internet ultrapassa fronteiras físicas, o que acarreta uma série de desafios à aplicação do direito penal. A atuação de agentes em diferentes países, com fuso horário e legislações distintas, dificulta a localização, identificação e punição dos culpados. Essa transnacionalidade dos crimes virtuais exige cooperação entre países e órgãos internacionais, como a Interpol e a Europol, bem como a constante atualização das normas jurídicas para abranger novas condutas criminosas digitais.

A motivação desses sujeitos ativos pode variar consideravelmente, desde interesses econômicos (como fraudes bancárias e extorsões) até fins ideológicos (como ataques hacktivistas, que visam chamar atenção para causas sociais ou políticas). Há ainda casos de espionagem corporativa ou estatal, nos quais agentes cibernéticos, muitas vezes patrocinados por governos, invadem redes adversárias para coletar informações estratégicas.

O crescimento da criminalidade na internet acompanha o avanço tecnológico e o aumento da dependência digital por parte da sociedade. À medida que mais aspectos da vida cotidiana migram para o ambiente virtual, como bancos, saúde, educação e relações interpessoais, surgem também novas oportunidades para ações delituosas. Nesse cenário, é essencial compreender quem são os autores desses crimes, suas estratégias e perfis, como forma de subsidiar políticas públicas eficazes de prevenção e combate.

Vale lembrar que o enfrentamento da criminalidade na internet não depende apenas da atuação repressiva. Investimentos em educação digital,

conscientização da população, capacitação de profissionais de segurança cibernética e reforço legislativo e institucional são medidas fundamentais para lidar com um fenômeno que se mostra cada vez mais dinâmico, técnico e globalizado.

1.2. VÍTIMAS MAIS AFETADAS

Embora a internet alcance diferentes faixas etárias, níveis educacionais e contextos socioeconômicos, alguns grupos têm se mostrado mais suscetíveis aos riscos cibernéticos. Entre eles, destaca-se a população idosa, que, nos últimos anos, tem aumentado significativamente sua presença no meio digital, impulsionada pelo desejo de manter vínculos sociais, acessar serviços online e conquistar maior autonomia. No entanto, essa mesma inclusão tecnológica, quando não acompanhada de suporte adequado, expõe os idosos a uma série de ameaças no ambiente virtual.

Uma pesquisa realizada pela Fundação Getúlio Vargas (FGV), com 68 idosos predominantemente do sexo masculino, demonstrou que os dispositivos mais utilizados por essa faixa etária são o celular e o computador, e que a familiaridade com os riscos digitais ainda é limitada. Entre os principais golpes identificados estão: o golpe do falso parente, o cartão clonado, a extorsão emocional, o falso empréstimo online, o roubo de identidade, a fraude por falsos funcionários e os enganos em compras virtuais. Tais golpes, muitas vezes, utilizam estratégias de engenharia social para explorar a confiança e a falta de domínio tecnológico dos idosos.

> “os idosos estão se tornando alvos mais frequentes de criminosos cibernéticos, apesar das dificuldades que enfrentam ao lidar com determinadas tecnologias. Isso se deve ao fato de que os idosos estão gradualmente adquirindo acesso às ferramentas tecnológicas, impulsionados pela percepção de que essas tecnologias podem proporcionar maior autonomia, bem-estar e integração social” (ALMEIDA, 2019; CORRÊA, 2022)

Além das barreiras tecnológicas, o processo de envelhecimento também pode acentuar vulnerabilidades nos aspectos emocionais, sociais e físicos,

tais como a solidão, a dependência de terceiros para atividades rotineiras e a redução das capacidades cognitivas. Esses fatores contribuem para que muitos idosos não consigam identificar comportamentos suspeitos ou reconhecer sinais de fraude, tornando-os alvos preferenciais dos cibercriminosos.

O impacto emocional decorrente da vitimização digital pode ser significativo, afetando não apenas a autoestima e a confiança do idoso em utilizar a internet, mas também sua saúde mental e seu sentimento de segurança. Por isso, é fundamental desenvolver ações educativas inclusivas, voltadas especificamente para esse público, a fim de capacitá-los quanto aos cuidados básicos de segurança digital, como não compartilhar dados pessoais, desconfiar de mensagens suspeitas e utilizar senhas seguras.

A dificuldade de adaptação às novas tecnologias é outro desafio crítico. Muitos idosos viveram grande parte de suas vidas sem contato direto com ferramentas digitais, o que torna a assimilação de conceitos como aplicativos, redes sociais, configurações de privacidade e autenticação em dois fatores mais complexa e, muitas vezes, intimidante. Por isso, treinamentos personalizados e o suporte contínuo oferecido por instituições públicas, ONGs, universidades e até familiares são indispensáveis para garantir que o processo de inclusão digital ocorra de forma segura e respeitosa.

Como alertam Miranda, Farias, Krug, Xavier e D'Orsi (2009; 2018), "apesar dos inúmeros benefícios que a internet pode oferecer, é fundamental estar ciente dos possíveis riscos envolvidos ao idoso. Dessa forma, é de extrema importância orientar os idosos a fazer uso da tecnologia de maneira segura e consciente, possibilitando que aproveitem todas as suas vantagens sem correrem riscos desnecessários".

Portanto, diante do avanço da criminalidade na internet, torna-se urgente ampliar o debate sobre os grupos mais vulneráveis às fraudes digitais, não apenas em termos de repressão aos crimes, mas sobretudo na prevenção e na promoção da cidadania digital. O idoso deve ser visto como sujeito de direitos também no meio virtual, e a sua segurança deve fazer parte das políticas públicas voltadas à inclusão tecnológica.

Estudos revelam que esse alto índice de vítimas da população idosa, se dá pela baixa familiaridade com a tecnologia e menor conhecimento com o mundo digital. Portanto, é necessário acompanhar a relação do idoso com a internet, como este contato ocorre e quais meios, o que está sendo feito e expor os riscos que corre.

Uma das principais dificuldades que os idosos enfrentam é a adaptação ao uso da tecnologia, um desafio que se torna ainda mais significativo quando se tem o primeiro contato com dispositivos digitais na terceira idade. Muitos idosos crescem em uma era onde a tecnologia avançada não fazia parte de suas rotinas, o que torna a compreensão de conceitos digitais, como aplicativos, internet e configurações de dispositivos, mais complexa e muitas vezes intimidadora. Por esse motivo, é essencial que os treinamentos e orientações voltados para essa faixa etária sejam cuidadosamente desenvolvidos, com um foco especializado que leve em conta as necessidades, limitações motoras, visuais e cognitivas, além da experiência de cada indivíduo.

1.3. ÍNDICES DE CRIMES VIRTUAIS (ANO 2023 – 2025)

O crime cibernético continua a crescer em escala e sofisticação em todo o mundo. Segundo estimativas do Statista - Cybercrime costs (2024), o custo global gerado por atividades criminosas online atingiu aproximadamente US$ 8,15 trilhões em 2023. Em 2024, esse valor subiu para US$ 9,22 trilhões, refletindo o impacto crescente desses delitos em governos, empresas e indivíduos. Para 2025, projeta-se que os prejuízos atinjam cerca de US$ 10,29 trilhões, com uma previsão para que em 2028 os prejuizos cheguem a marca de US$ 13,82 trilhões com uma taxa de crescimento anual composta (CAGR) estimada em 15% (STATISTA, 2024).

Entre os principais tipos de crimes cibernéticos, o phishing permanece como o mais recorrente. De acordo com dados da Cybersecurity Ventures (2023), foram registrados quase 9 milhões de casos globalmente apenas no último ano. Em seguida, destaca-se a violação de dados pessoais, com aproximadamente 1,66 milhão de incidentes, seguida das fraudes em

pagamentos e entregas, que contabilizaram cerca de 1,5 milhão de ocorrências (CYBERSECURITY VENTURES, 2023).

No cenário brasileiro, a situação também é preocupante. Conforme apontado por uma pesquisa do DataSenado (2024), cerca de 24% da população brasileira com mais de 16 anos foi vítima de golpes digitais nos últimos 12 meses. Isso representa mais de 40,85 milhões de pessoas que sofreram perdas financeiras em decorrência de crimes cibernéticos (DATASENADO, 2024).

Esse panorama evidencia a crescente necessidade de investimentos em cibersegurança, bem como a importância da educação digital da população para reconhecer e evitar tentativas de golpe na internet. Governos, empresas e usuários devem atuar conjuntamente para mitigar os riscos e fortalecer a proteção no ambiente digital.

Segundo o wired - Cybersegurity in Financial Sevices, o setor financeiro é um dos mais visados pelos cibercriminosos, devido a alta movimentação de transações e natureza crítica dos dados financeiros. O ataque a instituições financeiras e bancos tem sido o foco central, já que a possibilidade de roubo de fundos ou de dados pessoais e bancários pode ser altamente lucrativo para os criminosos.

Os ataques de ransomware e fraudes financeiras, incluindo fraudes de pagamentos e roubo de informações bancárias tenham causado mais de US$ 30 bilhões de perdas em 2023.

O setor financeiro depende totalmente da confiança do consumidor, sendo assim sofrendo com ataques cibernéticos, como roubo de dados bancários, as instituições podem perder a confiança dos seus cliente, o que acaba levando os clientes a buscarem outras instituições que as deixem se sentir mais seguras.

O custo de recuperação é regulação, após um ataque cibernético é alto, tendo

em vista a recuperação dos sistemas comprometidos, reforços da segurança cibernética e novas medidas regulatórias, em alguns países os governos exigem que as instituições invistam fortemente em sua segurança cibernética, o que normalmente leva a custos operacionais. (WIRED - CYBERSECURITY IN FINANCIAL SEVICES, 2023)

O setor da saúde também é um grande alvo dos crimes cibernéticos, muito em vista por esse setor ser particularmente vulnerável, pois lida com dados sensíveis como informações de saúde, histórico médico e dados seguros, nas quais podem ser utilizadas para os criminosos entrarem em contato pedindo valores para determinados exames ou medicamentos.

Um ataque no setor da saúde pode ser devastador já que um ataque a um hospital ou rede de saúde pode interromper o atendimento de pacientes por dias ou até semanas, podendo causa danos à saúde de pacientes.

O roubo de dados pessoais e informações da saúde é uma grande preocupação, pois no mercado negro elas tem um valor alto. A violação pode resultar em multas pesadas , especialmente com regulamentações como a lei de portabilidade e responsabilidade de seguro de saúde (HIPAA) nos Estados Unidos.

O setor da saúde está sujeito a regulamentações mais rigorosas em termos de dados pessoais. (HEALTHCARE IT NEWS – CYBERSECURITY IN HEALTCARE, 2023)

2. TIPOS DE CRIMES CIBERNÉTICOS

A criminalidade na internet tem se diversificado de forma acelerada, acompanhando o desenvolvimento tecnológico e a popularização dos dispositivos digitais. Com isso, surgiram diferentes formas de delitos praticados em ambientes virtuais, cujas características e impactos variam conforme os meios utilizados, os bens jurídicos atingidos e o grau de complexidade da infração. Para facilitar o estudo e a repressão desses crimes, especialistas em

direito digital e segurança da informação desenvolveram classificações específicas que ajudam a identificar suas tipologias e consequências legais.

Segundo Garcia, Madacar e Luciano (2018), os crimes cibernéticos podem ser classificados em crimes puros, mistos e comuns, bem como em crimes próprios e impróprios, considerando aspectos como o alvo da ação criminosa, o uso indispensável da tecnologia, o tipo de dano causado e o enquadramento jurídico.

2.1. CRIMES PUROS, MISTOS E COMUNS

Esta classificação baseia-se na relação entre o crime e o ambiente digital, observando se a tecnologia é apenas um meio de execução ou o próprio fim do delito.

Crimes puros (ou próprios do ciberespaço): São aqueles em que a infração ocorre exclusivamente no ambiente digital, sendo a tecnologia não apenas o meio, mas também o objeto da ação criminosa. O alvo do crime é o próprio sistema, dado ou rede. São exemplos: *ataques de negação de serviço (DDoS)*, *disseminação de malwares*, *hacking* e *destruição de dados*. Essas práticas visam comprometer a integridade, confidencialidade ou disponibilidade dos sistemas informáticos.

Crimes mistos (ou híbridos): Nessa categoria, o meio digital é essencial para a execução da conduta ilícita, mas o bem jurídico atingido pode estar fora do ciberespaço. Por exemplo, em casos de *fraudes bancárias online*, *roubo de identidade digital* ou *phishing*, o agente utiliza ferramentas digitais para atingir objetivos no mundo real, como obter vantagens econômicas ou acesso a dados sensíveis.

Crimes comuns (ou tradicionais com suporte digital): São delitos já previstos no Código Penal brasileiro, mas que passaram a ser praticados com o uso de recursos tecnológicos, ampliando seu alcance e dificultando sua repressão. Entre eles estão *ameaças*, *calúnia*, *difamação*, *injúria*, *extorsão* e *estelionato*.

O diferencial está na forma como são cometidos: por meio de redes sociais, aplicativos de mensagens, e-mails ou outras plataformas virtuais.

Essas classificações permitem compreender como o ambiente virtual pode ser tanto o campo de atuação quanto o instrumento facilitador da criminalidade, revelando a necessidade de atualização constante das estratégias de combate e da legislação penal.

2.2. CRIMES PRÓPRIOS E IMPRÓPRIOS

Outra importante distinção nos estudos sobre crimes cibernéticos é aquela proposta por Crespo (2015), que classifica essas infrações em crimes próprios (ou puros) e crimes impróprios (ou mistos), a partir da natureza do bem jurídico violado.

> "Crimes digitais próprios ou puros (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (*hacking*), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas; e Crimes digitais impróprios ou mistos (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc). São exemplos de crimes digitais impróprios os contra a honra praticados na Internet, as condutas que envolvam trocas ou armazenamento de imagens com conteúdo de pornografia infantil, o estelionato e até mesmo o homicídio" (CRESPO, 2015).

Os crimes cibernéticos próprios envolvem ações diretamente voltadas contra os sistemas informáticos ou seus componentes. São considerados delitos de risco informático, pois colocam em perigo a segurança de informações, redes ou dispositivos, como: invasão de sistemas sem autorização; destruição ou alteração de dados; distribuição de vírus ou outros programas maliciosos; interferência no funcionamento de redes corporativas ou governamentais.

Tais condutas visam diretamente o ambiente digital, podendo comprometer

estruturas sensíveis, como bancos de dados governamentais, servidores públicos e plataformas financeiras.

Por outro lado, os crimes virtuais impróprios:

Crimes cibernéticos impróprios referem-se àquelas condutas criminosas tradicionais que, embora não tenham como alvo direto a tecnologia, são executadas por meio dela. Ou seja, o crime pode ser praticado por qualquer meio, mas ganha contornos específicos e potencial agravamento ao ocorrer no ambiente digital.

> "estelionato e furto eletrônicos (fraudes bancárias), invasão de dispositivo informático e furto de dados, falsificação e supressão de dados, armazenamento; produção; troca; publicação de vídeos e imagens contendo pornografia infanto juvenil (arts. 241 e 241-A, do ECA - Lei nº 8.069/1990), assédio e aliciamento de crianças (art. 241-D, do ECA - Lei nº 8.069/1990, ameaça, *cyberbullying* (veiculação de ofensas em blogs e comunidades virtuais), incitação e apologia de crime, prática ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, venda ilegal de medicamentos"

Essa categoria de crimes revela como o meio digital pode potencializar a gravidade dos delitos, facilitando a disseminação, a escalabilidade e o anonimato dos agressores. Um ataque praticado virtualmente pode atingir milhares de pessoas em diferentes regiões ao mesmo tempo, exigindo uma abordagem mais eficaz por parte das autoridades.
Além disso, o uso de técnicas sofisticadas como *criptografia*, *VPNs*, *deep web* e *spoofing* dificulta o rastreamento e a responsabilização dos autores, o que evidencia a urgência de aprimoramentos legais e operacionais.

3. EVOLUÇÃO LEGISLATIVA E LEIS PARA O COMBATE AOS CRIMES VIRTUAIS.

> "Os crimes digitais, cada vez mais comuns no nosso cotidiano, passaram a contar com mais algumas normas que tipificam condutas antes irrelevantes para o Direito Penal."

(CRESPO, 2015)

Pode se dizer que o marco das leis implantadas para o combate aos crimes virtuais se deu a partir de 2012. A crescente digitalização da sociedade trouxe consigo uma série de desafios legais, especialmente no que tange à proteção contra crimes cibernéticos. A legislação brasileira evoluiu para enfrentar essas novas ameaças, com destaque para três marcos legais fundamentais: a Lei nº 12.735/2012, a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e a Lei nº 12.965/2014 (Marco Civil da Internet).

Lei nº 12.735/2012 – Combate ao Racismo na Internet:

Sancionada em 2012, a Lei nº 12.735/2012 estabelece medidas para combater o racismo na internet. Ela determina a obrigatoriedade de interrupção imediata de mensagens com conteúdo racista e sua retirada de qualquer meio de comunicação. Além disso, a lei prevê a criação de delegacias virtuais especializadas no enfrentamento de crimes cibernéticos relacionados ao racismo.

Essa legislação representa um avanço significativo na proteção contra crimes de ódio online, refletindo a necessidade de adaptação da legislação penal às novas formas de manifestação discriminatória no ambiente digital.

Lei nº 12.737/2012 – Lei Carolina Dieckmann:

A Lei nº 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, foi sancionada em resposta ao vazamento de fotos íntimas da atriz Carolina Dieckmann. Ela introduziu alterações no Código Penal Brasileiro, tipificando crimes informáticos específicos, como a invasão de dispositivos eletrônicos e a divulgação não autorizada de conteúdos privados.

O artigo 154-A do Código Penal, inserido por essa lei, tipifica a invasão de dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo.

Além disso, a lei prevê penas mais severas para casos em que a invasão resulte em prejuízo econômico à vítima, aumentando a pena de detenção de três meses a um ano para reclusão de um a quatro anos, conforme alterações posteriores.

3.1. O MARCO CIVIL DA INTERNET

Após o aumento dos casos de crimes cibernéticos, também houve o MCI (Marco Civil da Internet) que permitiu a investigação de diversos crimes cibernéticos, estabelecendo princípios, garantias direitos e deveres para o uso da Internet, pensando em um contexto geral, os provedores de conexão também foram estabelecidos limites através da Lei nº 12.965/2014, na qual regula o uso da internet a nível nacional.

O MCI tem como objetivo:

> [...] teve por objetivo estabelecer princípios, garantias, direitos e deveres para o uso da Internet, cujo acesso é considerado um direito do cidadão. Sua criação teve importância ímpar na regulação das relações digitais, especialmente no que tange a: inclusão digital (art. 27); exigência de neutralidade da rede (art. 9º), evitando, assim, a discriminação da informação; proteção à intimidade e ao sigilo dos dados (art. 7º, I, II, III), inclusive com a exigência de consentimento expresso do usuário para a coleta, o uso, o armazenamento e o tratamento de dados pessoais (art. 7º, IX); e garantia da liberdade de expressão, como fundamento do uso da Internet no Brasil (art. 2º). O detalhamento de garantias consumeristas aplicáveis às relações no ambiente digital também é um ponto positivo da norma (vide art. 7º, IV a VIII e XI a XIII). (COSTA, 2016)

Entre os principais pontos da lei, destacam-se:

Neutralidade da rede: Garante que os provedores de internet tratem de forma isonômica quaisquer pacotes de dados, sem discriminação por conteúdo, origem, destino, serviço, terminal ou aplicação. Isso impede práticas como a cobrança diferenciada por tipo de conteúdo ou a redução da velocidade de acesso a determinados serviços.

Proteção à privacidade e aos dados pessoais: Assegura a inviolabilidade da intimidade e da vida privada, bem como o sigilo das comunicações pela internet. Estabelece que os dados pessoais só podem ser coletados, utilizados e armazenados mediante consentimento expresso do usuário.

Responsabilidade dos provedores: Define as responsabilidades dos provedores de conexão e de aplicações de internet, incluindo a obrigação de manter registros de acesso a aplicações de internet pelo prazo de um ano, para fins de investigação e repressão de crimes.

Liberdade de expressão: Garante a liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal, assegurando que a internet continue sendo um ambiente democrático e aberto.

3.2. PROBLEMÁTICAS PARA COMBATER O CRIME VIRTUAL

Para que a sanção penal possa ser aplicada deve haver certezas e provas do crime praticado, caso não seja comprovado o juiz poderá absolver o réu, como menciona o artigo 388 do Código Processual Penal.

> Art. 386. O juiz absolverá o réu, mencionando a causa na parte dispositiva, desde que reconheça: I - Estar provada a inexistência do fato; II - Não haver prova da existência do fato; III - Não constituir o fato infração penal;IV - Estar provado que o réu não concorreu para a infração (...) V - Não existir prova de ter o réu concorrido para a infração penal

As empresas de informação também vem sendo alvo das problemáticas ao combate, onde por muitas vezes se recusam a contribuir auxiliando a polícia e ao judiciário, como por exemplo, o Whatsapp, especialmente em casos que envolvem a divulgação de dados pessoais ou a violação da privacidade dos usuários. A falta de regulamentação específica sobre a cooperação entre empresas de tecnologia e autoridades judiciais também contribui para a morosidade na resolução de casos.

Apesar dos avanços legislativos, o combate aos crimes virtuais enfrenta desafios significativos. A rápida evolução tecnológica e a sofisticação dos ataques cibernéticos dificultam a aplicação efetiva das leis existentes.

Um dos principais obstáculos é a dificuldade de identificação e responsabilização dos infratores, que frequentemente utilizam ferramentas para ocultar sua identidade e localização. Além disso, a colaboração internacional é essencial, uma vez que muitos crimes cibernéticos transcendem fronteiras nacionais.

Contudo, apesar das alterações realizadas, os demais crimes até hoje são julgados com base o efeito danoso, a partir disto é notório a dificuldade na real

punição destes infratores, uma vez que deve ser traçado como chegará ao infrator. O que vem causado na população a sensação de falta de punição ou até mesmo inexistência das leis estabelecidas.

Pois o volume de crimes que ocorrem no país, supera a o número de capacitados para realizar as investigações, conforme afirmou Carlos Eduardo Sobral, chefe da unidade de Repressão a Crimes Cibernéticos da Policia Federal na CPI dos Crimes Cibernéticos, realizada no dia 20/08/2014 "O volume de investigação vem crescendo, e o efetivo tem que crescer na mesma proporção. Hoje o nosso efetivo acaba sendo menor do que o volume que necessita para que seja dado um rápido andamento às investigações" (apud. Canuto, Luiz Cláudio, 2015).

3.3. PERSPECTIVAS FUTURAS

O Brasil tem evoluído em sua legislação para enfrentar os crimes cibernéticos. Recentemente, a Comissão de Comunicação e Direito Digital do Senado analisou o Projeto de Lei 3.085/2024, que propõe o aumento das penas para crimes cibernéticos cometidos contra figuras públicas. A proposta visa ampliar a proteção legal, considerando agravantes como o uso de inteligência artificial, reincidência e a natureza pública da vítima. Se aprovado, o projeto poderá aumentar em até 70% a pena para tais infrações, desestimulando práticas criminosas cada vez mais sofisticadas no ambiente digital .

A natureza global da internet exige uma abordagem colaborativa entre países para o combate eficaz aos crimes cibernéticos. A Convenção de Budapeste, ratificada por diversos países, incluindo o Brasil, estabelece diretrizes para a cooperação internacional em matéria de crimes cibernéticos. No entanto, a aplicação uniforme dessa convenção enfrenta desafios devido às diferenças nas legislações nacionais e à complexidade das investigações transnacionais. Além disso, a utilização de tecnologias como criptografia e anonimato por criminosos dificulta a identificação e responsabilização dos infratores. A cooperação entre órgãos de diferentes países e a harmonização das legislações são essenciais para superar essas barreiras e garantir a eficácia das investigações.

Algumas ações estão em validação para contribuir ao combate da

criminalidade na internet, dentre elas podemos destacar a própria internet, através da implementação de tecnologias avançadas, como autenticação multifatorial, criptografia robusta e sistemas de detecção baseados em inteligência artificial, será fundamental para prevenir e mitigar os efeitos dos crimes cibernéticos. A integração dessas tecnologias no cotidiano das organizações e dos usuários pode criar barreiras adicionais que dificultam a ação de criminosos.

A educação digital também desempenha um papel crucial na prevenção de crimes cibernéticos. É necessário promover a conscientização sobre os riscos associados ao uso da internet e fornecer treinamento adequado para que os usuários possam identificar e evitar práticas fraudulentas. Além disso, é importante que as pessoas compreendam seus direitos e responsabilidades no ambiente digital, fortalecendo a cultura de segurança online.

Dada a velocidade com que as tecnologias evoluem, é essencial que a legislação acompanhe essas mudanças. A criação de normas flexíveis e adaptáveis permitirá que o sistema jurídico responda de forma eficaz às novas formas de crimes digitais. Além disso, a colaboração entre legisladores, especialistas em tecnologia e representantes da sociedade civil poderá contribuir para a elaboração de políticas públicas mais eficazes no combate à criminalidade na internet.

CONSIDERAÇÕES FINAIS

O estudo sobre a criminalidade no contexto tecnológico se mostra em um cenário complexo e desafiador. A evolução digital trouxe não apenas benefícios à sociedade, como a facilitação das relações humanas e o acesso à informação, mas também ampliou as possibilidades de crimes virtuais, que hoje se configuram como um grande problema global. A crescente utilização da internet, a anonimização dos usuários e o desenvolvimento de tecnologias como redes privadas virtuais (VPNs) e criptografia dificultam a identificação dos infratores e a aplicação de punições eficazes.

A análise dos diferentes tipos de crimes cibernéticos, como os crimes puros, mistos, comuns, próprios e impróprios, demonstra as diferentes formas do crime no ambiente digital. Esses crimes atingem uma ampla gama de vítimas, com destaque para os idosos, que, devido à baixa familiaridade com a tecnologia, se tornam alvos fáceis de cibercriminosos. É essencial, portanto, que haja um investimento contínuo em campanhas de conscientização e formação digital para esse público, a fim de protegê-los de riscos e golpes virtuais. No entanto, é dever do Estado garantir a proteção de todos, com especial atenção às vítimas mais vulneráveis, como os idosos no ambiente digital. É fundamental destacar a importância da educação digital, que visa capacitar os indivíduos para assumir responsabilidades e reduzir as infrações cibernéticas, especialmente aquelas direcionadas aos idosos. É crucial também enfatizar a diversidade de golpes digitais existentes e sua crescente ameaça a esse público.

Apesar da evolução das leis brasileiras, como o Marco Civil da Internet e as leis específicas contra crimes cibernéticos, ainda existem grandes desafios para o combate à criminalidade digital. A falta de recursos adequados para as investigações, aliada à complexidade dos crimes virtuais, contribui para a sensação de impunidade e dificulta a resolução desses delitos de maneira ágil e eficaz.

Somente por meio de uma ação conjunta será possível aprimorar as estratégias de combate a crimes cibernéticos e garantir a proteção dos direitos dos cidadãos no ambiente digital.

Em suma, a luta contra a criminalidade no contexto tecnológico exige um esforço contínuo de todos os setores da sociedade, incluindo governo, empresas e cidadãos, para que se possa garantir um ambiente digital mais seguro e confiável para todos.

REFERÊNCIAS BIBLIOGRAFICAS

CARVALHO, Patricia 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, Pouso Alegre, 2017. Disponível em: https://www.fdsm.edu.br/adm/artigos/6917c36392274c9b6393c7f7a7bddbd1.pdf. Acesso em: 24/03/2025.

COSTA, Luiz Fernando. **A tipificação dos crimes cibernético: uma análise da adequação das leis existentes para lidar com os desafios e especificidades dos crimes cometidos no ambiente digital**. Belo Horizonte, 2023. Disponível em: https://repositorio-api.animaeducacao.com.br/server/api/core/bitstreams/91db55fb-8f94-42e5-bf19-e0fab1a144b8/content. Acesso em: 24/03/2025

CRUZ, Diego; Rodrigues, Juliana. **Crimes cibernéticos e a falsa sensação de impunidade**. Revista científica eletrônica do concurso de Direito, 13º edição, 2018. Disponível em:https://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso em: 24/03/2025.

GONÇALVES BARRETO, Alesandro. **Efetividade da ordem judicial em desfavor de provedores de conexão e aplicações de internet: sanções do art. 12 do Marco Civil da Internet.** Revista Eletrônica Direito & TI, v. 1, n. 1, p. 6, 2015. Disponível em: https://direitoeti.com.br/direitoeti/article/view/11. Acesso em: 24/03/2025.

MENDES, Marcelo Doval. **O Marco Civil da Internet no Brasil: direitos, deveres e programas.** Revista Direitos Humanos Fundamentais, v. 15, n. 1, 2015. Disponível em: https://revistas.unifieo.br/rmd/article/view/1044. Acesso em: 24/03/2025

RAMOS, Jonathas Cordeiro. **Os crimes praticados na interne**t. Site Unaerp, Ribeirão Preto, 2019. Disponível em: https://www.unaerp.br/documentos/3538-rci-os-crimes-praticados-na-internet-dez-2019/file. Acesso em: 24/03/2025.

SANTOS, Matheus Guedes et al. **Crimes e golpes virtuais: desafios enfrentados pelos idosos na era tecnológica**. Revista observatorio de la economia Latinoamericana, Curitiba, volume 21, n. 9, 2023. Disponível em: https://ojs.observatoriolatinoamericano.com/ojs/index.php/olel/article/download/1293/1034/3826#:~:text=Entre%20aqueles%20que%20foram%20v%C3%ADtimas,contas%20de%20cart%C3%A3o%20e%20cheques.. Acesso em: 29/01/2025.

SILVA, Emanuely Costa; CUNHA, Raíla Silva. **Crimes Cibernéticos e investigação policial**. Revista eletrônica do Ministério Público do Estado do Piauí, edição 02, 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 24/03/2025

SOUZA, Lucas Daniel Ferreira; DE LUCA, Guilherme Domingos. **Lei 12.965/2014: democratização da internet e efeitos do marco civil na sociedade da informação**. Revista Paradigma, n. 23, 2014. Disponível em: https://revistas.unaerp.br/paradigma/article/view/466. Acesso em: 24/03/2025.

STEFANI, Ailton et al. **A vulnerabilidade social de idosos frente a golpes no âmbito digital.** Research, society and development, volume 11, n. 11, 2022. Disponível em: https://www.researchgate.net/publication/363064431_A_vulnerabilidade_social_de_idosos_frente_a_golpes_no_ambito_digital. Acesso em: 29/01/2025

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

https://www.revistas.usp.br/eav/article/view/115093. Acesso em: 29/01/2025

ZACARIAS, Fabiana; ZACHARIAS, Lucas Freire. **Crimes virtuais: análise das dificuldades e limitações ao combate**. Revista jures, volume 16, n. 29, p. 29- 61, 2023. Disponível em: https://estacio.periodicoscientificos.com.br/index.php/juresvitoria/article/download/1537/1628/2822. Acesso em: 30/01/2025