UNIVERSIDADE CATÓLICA DO SALVADOR
FACULDADE DE DIREITO
BACHARELADO DE DIREITO

OS AVANÇOS DOS CRIMES CIBERNÉTICOS E A LACUNA EXISTENTE NA LEGISLAÇÃO BRASILEIRA

LUCAS MACEDO CABRAL

SALVADOR
2025

LUCAS MACEDO CABRAL

OS AVANÇOS DOS CRIMES CIBERNÉTICOS E A LACUNA EXISTENTE NA LEGISLAÇÃO BRASILEIRA

Trabalho de Conclusão de Curso apresentado à Universidade Católica do Salvador, como requisito parcial para a obtenção do Título de Graduado em Direito.

Orientador: Ms. Cristiano Lázaro

SALVADOR

2025

FICHA DE APROVAÇÃO

Trabalho de conclusão de curso aprovado como requisito parcial para obtenção do grau de Bacharel em Direito da Universidade Católica do Salvador.

Lucas Macedo Cabral

Acadêmico

Cristiano Lázaro

Professor Orientador

Salvador,_____ de _____de 2025.

RESUMO

Com o avanço da tecnologia e a popularização da internet, surgiram novas formas de criminalidade no ambiente virtual, conhecidas como crimes cibernéticos. Essas práticas, que afetam indivíduos, empresas e instituições, representam um desafio crescente para o ordenamento jurídico. A escolha do tema se justifica pela frequência e complexidade dos delitos digitais, que muitas vezes não encontram respostas eficazes na legislação atual. Diante disso, o problema central desta pesquisa é: como a legislação brasileira tem enfrentado os crimes cibernéticos e quais são suas limitações na punição dos infratores? Para responder a essa questão, adota-se como metodologia a revisão bibliográfica, com base em obras jurídicas, artigos científicos e documentos oficiais. O objetivo geral é analisar os desafios legais no combate aos crimes cibernéticos no Brasil. Como objetivos específicos, busca-se: entender os conceitos e a evolução histórica dos crimes digitais; identificar os principais delitos cometidos pela internet; traçar o perfil dos criminosos; e discutir as falhas legais e punitivas. O trabalho está estruturado em quatro capítulos: o primeiro trata dos conceitos e da historicidade dos crimes cibernéticos; o segundo apresenta os principais delitos virtuais; o terceiro analisa o perfil do infrator; e o quarto discute as insuficiências legais e os desafios enfrentados pela Justiça.

Palavras-chave: Crimes Cibernéticos. Internet. Responsabilidade penal.

ABSTRACT

With the advancement of technology and the popularization of the internet, new forms of crime have emerged in the virtual environment, known as cybercrimes. These practices, which affect individuals, companies, and institutions, represent a growing challenge for the legal system. The choice of this topic is justified by the frequency and complexity of digital offenses, which often do not find effective responses in current legislation. Given this, the central problem of this research is: how has Brazilian legislation addressed cybercrimes, and what are its limitations in punishing offenders? To answer this question, a bibliographic review methodology is adopted, based on legal works, scientific articles, and official documents. The general objective is to analyze the legal challenges in combating cybercrimes in Brazil. As specific objectives, the study seeks to understand the concepts and historical evolution of digital crimes; identify the main offenses committed via the internet; profile the criminals involved; and discuss the legal and punitive shortcomings. The work is structured into four chapters: the first addresses the concepts and historicity of cybercrimes; the second presents the main virtual offenses; the third analyzes the offender's profile; and the fourth discusses the legal insufficiencies and challenges faced by the justice system.

Keywords: Cybercrimes. Internet. Criminal liability.

SUMÁRIO

1 INTRODUÇÃO

Nas últimas décadas, a revolução digital transformou profundamente a forma como as pessoas se comunicam, trabalham, consomem informações e realizam transações comerciais. Com a expansão da internet e o avanço das tecnologias da informação, surgiu um novo espaço social: o ciberespaço. No entanto, juntamente com as inúmeras oportunidades proporcionadas por esse ambiente virtual, emergiram também novos desafios, entre eles os crimes cibernéticos. Essas práticas delituosas, que se utilizam da rede mundial de computadores como meio ou como fim, representam uma ameaça significativa à segurança individual, institucional e até mesmo nacional.

A relevância do tema se justifica pela crescente incidência e sofisticação dos crimes cometidos por meios digitais, que vão desde fraudes financeiras até ataques cibernéticos complexos a infraestruturas críticas. A legislação, por sua vez, tem enfrentado dificuldades para acompanhar a evolução tecnológica e para garantir a responsabilização efetiva dos criminosos. Diante desse cenário, torna-se fundamental compreender a natureza e as implicações dos crimes cibernéticos, bem como os obstáculos enfrentados pelo sistema jurídico na tentativa de coibir e punir tais condutas.

A problemática que norteia este trabalho consiste na seguinte questão: como a legislação brasileira tem enfrentado os desafios impostos pelos crimes cibernéticos e quais são as principais limitações na punição dos infratores nesse contexto digital?

A metodologia utilizada para a realização desta pesquisa é a revisão bibliográfica, a partir da análise de livros, artigos científicos, legislações pertinentes e documentos oficiais que tratam do tema. Essa abordagem permite reunir o conhecimento já produzido sobre o assunto, identificar lacunas existentes na literatura e propor reflexões críticas a respeito das medidas legais adotadas no combate aos delitos cibernéticos.

Diante disso, este estudo tem como objetivo geral analisar os desafios enfrentados pelo ordenamento jurídico brasileiro no combate aos crimes cibernéticos, com foco nas limitações legais, na eficácia das punições e na evolução normativa diante das novas demandas tecnológicas. Como objetivos específicos, pretende-se: compreender os conceitos fundamentais e a trajetória histórica dos crimes cibernéticos; identificar e classificar os principais delitos cometidos por meio da internet; traçar o perfil dos indivíduos que praticam esses crimes, considerando aspectos sociais, comportamentais e psicológicos; e, por fim, avaliar a suficiência das punições previstas na legislação brasileira e os entraves legais enfrentados na sua aplicação prática.

O presente trabalho está dividido em quatro capítulos. O Capítulo 1, intitulado "Crimes Cibernéticos: Conceitos e Historicidade", apresenta uma definição do que são crimes cibernéticos, traçando um panorama histórico de seu surgimento e evolução, bem como as primeiras respostas jurídicas às novas modalidades delitivas. O Capítulo 2, "Delitos Cometidos através da Internet", explora as principais formas de crimes cibernéticos, como invasão de dispositivos, fraudes eletrônicas, disseminação de conteúdos ilícitos e outros atos ilícitos praticados no ambiente digital. O Capítulo 3, "Perfil do Criminoso", discute as características, motivações e comportamentos dos indivíduos que cometem crimes cibernéticos, incluindo aspectos sociológicos e psicológicos. Por fim, o Capítulo 4, intitulado "Insuficiência de Punições e Desafios Legais", analisa as dificuldades enfrentadas pelo ordenamento jurídico brasileiro na repressão eficaz a esses crimes, apontando a necessidade de atualização legislativa.

2. CRIMES CIBERNÉTICOS: CONCEITOS E HISTORICIDADE

A humanidade tem passado por profundas transformações nas últimas décadas. Inúmeros fatores têm contribuído para esse acontecimento. Mas, sem dúvida nenhuma, o que mais tem influenciado no comportamento humano são as TICs. Tecnologias de Informação e Comunicação (TICs) são o conjunto de ferramentas relacionadas à transmissão, processamento e armazenamento digitalizado de informações.

As formas de se comunicar, de expor os pensamentos, de trabalhar, de se relacionar, inclusive afetivamente, de compra e venda de produtos, mudaram-se radicalmente com o advento das citadas TICs. E, inevitavelmente, surgiram novos crimes e novas formas de cometimento de crimes. No século XIX, Emile Durkheim já observou que onde há sociedade há crime. Constata Durkheim (1999) que, em qualquer sociedade, seja de qualquer tipo e de qualquer época, haverá crime. O delito faz parte da vida coletiva, segundo o renomado sociólogo.

O surgimento da internet e o uso generalizado de computadores proporcionou novos caminhos a serem explorados pelos criminosos. Os crimes cibernéticos referem-se a atividades criminosas realizadas através do uso de redes de computadores ou da Internet. Estes crimes não são limitados por fronteiras físicas e podem ser realizados de qualquer lugar do mundo com acesso à Internet. Conforme afirma Robert Spadinger:

> A Internet é onipresente, seja na vida individual, como entretenimento ou forma de comunicação, seja nas corporações ou até nos serviços públicos

> governamentais. Nos próximos anos, se assistirá à continuada escala da Internet e de todos os serviços conjugados em todos os setores. O mundo se transforma a cada dia mais em uma grande Rede, cada vez maior, mas conectada, disponível em qualquer lugar e em qualquer aparelho com o qual se realiza uma infinidadede atividades pessoais e profissionais (SPADINGER, 2012, p. 65).

Os crimes virtuais são atos criminosos cometidos através do uso de tecnologias digitais, tais como internet, computadores, smartphones e outros dispositivos eletrônicos. Com o uso crescente da tecnologia, os cibercrimes se tornaram mais comuns e sofisticados, representando ameaças significativas para indivíduos, organizações e governos. Alguns tipos comuns de crimes cibernéticos incluem hacking, cyberstalking, roubo de identidade, phishing, cyberbullying e resgates. Estes crimes podem causar perdas financeiras substanciais, danos à reputação e angústia emocional às vítimas.

Os criminosos cibernéticos frequentemente usam uma série de técnicas para perpetrar seus crimes, tais como *malware*, engenharia social e ataques de negação de serviço. Eles podem visar indivíduos, empresas ou mesmo Estados-nação, e são motivados por vários fatores, tais como ganho financeiro, motivos políticos ou vinganças pessoais.

Se a vida coletiva se transformou radicalmente, os crimes também acompanharam essa mudança. Nesse contexto é que surge o conceito de cibercriminalidade, ou, de forma ampla, crimes cometidos através das tecnologias de informação e comunicação, sendo as tecnologias meio ou objeto do crime. Conforme conceitua Manzur e Pinheiro:

> Todas aquelas ações ou omissões típicas, antijurídicas e dolosas, trate-se de fatos isolados ou de um série deles, cometidos contra pessoas naturais ou jurídicas, realizadas em uso de um sistema de tratamento da informação e destinadas a produzir um prejuízo na vítima através de atentados à sã técnica informática, o qual, geralmente, produzirá de maneira colateral lesões a distintos valores jurídicos, reportando-se, muitas vezes, um benefício ilícito no agente, seja ou não seja de caráter patrimonial, atue com ou sem ânimo de lucro(MANZUR; PINHEIRO, 2000, p. 18/19).

A transformação da sociedade, caracterizada pela sociedade líquida e de risco, conforme teorizações de Zigmunt Bauman (BAUMAN, Z, 2001) e Ulrich Beck (BECK, U. 1998 e 2018), transformou as relações sociais, de modo que grande parte das ações humanas se realizam no ciberespaço. Se é cediço que “onde há sociedade, há crime”, temos que reconhecer que no ciberespaço há ainda mais. E crescem vertiginosamente no Brasil e no mundo. Segundo Barrió Andrés apresenta dados que demonstram que os crimes cibernéticos têm representado 0,8 por cento do PIB mundial (BARRIO ANDRÉS, M. 2008, p 28).

Segundo Damásio e José Milagre, o Brasil é o quarto maior alvo de crackers em ataques de pishing do mundo, figurando entre os cinco países que mais tiveram empresas

hackeadas, com 38 milhões de usuários lesados (JESUS, D. MILAGRE, J. A. 2006, p 27). Os criminosos passaram a se aproveitar do fato das pessoas estarem mais em casa, usando a internet, para ler notícias, procurar informações e para comprarem mais pela internet para aplicarem mais golpes.

Importante compreendermos em que cenário social esse fenômeno se insere. A cibercriminalidade está intimamente ligada à nova "sociedade de informação" ou à chamada modernidade líquida, cunhada por Zigmunt Bauman (2001), ou à chamada sociedade de risco, teorizada por Ulrich Bech (2018). Criador e criatura se entrelaçam: os crimes cibernéticos são fruto da sociedade de informação, e a sociedade da informação propiciou a criação de novos bens jurídicos, quais sejam, os próprios dados, ambientes e espaços virtuais a serem atacados.

Machado (2010), comentando acerca dos crimes cibernéticos, faz relevante alerta sobre a potência da popularização das máquinas, observando que a sociedade da informação teve sua potência elevada com a popularização das máquinas e suas conexões, levando a boa parte da população o acesso a um cotidiano com características próprias e com arquivos intangíveis como tema de sua existência e sustentabilidade. A rede mundial de computadores trouxe a velocidade aos relacionamentos (comerciais, negociais, humanos, internacionais etc) e dissolveu fronteiras físicas, permitindo que o usuário-internauta experimentasse liberdade em grau antes inimaginável. Isto posto, aponta também as principais práticas criminosas na atualidade no mundo digital.

Além disso, as agências de aplicação da lei e os sistemas judiciais muitas vezes lutam para acompanhar a rápida evolução da tecnologia, levando a uma falta de pessoal devidamente treinado e leis ultrapassadas. Isto pode resultar em processos judiciais ineficazes e sentenças inadequadas para os criminosos cibernéticos. Deve-se priorizar a proteção dos sistemas e dispositivos digitais, assim como priorizamos a proteção da propriedade física e das vidas. Somente então poderemos esperar deter efetivamente o crime cibernético e responsabilizar aqueles que o cometem por suas ações.

Segundo Shoueri (2001, p. 21/22), consiste em assegurar a privacidade, a identidade da autoria, a inalterabilidade de conteúdo, enfim, a segurança na celebração dos contratos virtuais é que surgiu a criptografia, espécie de assinatura codificada, regulada pela criptologia, representativa da codificação de informações de forma apta a impedir a interceptação não desejada, por meio de convenções secretas às partes contratantes e às testemunhas.

Para combater os cibercrimes, é essencial ter medidas de segurança adequadas,

como senhas fortes, firewalls e software antivírus. É também crucial educar nós mesmos e outros sobre os vários tipos de crimes cibernéticos e seu impacto. Alguns tipos comuns de crimes cibernéticos incluem roubo de identidade, phishing scams, hacking e ataques de malware.

O roubo de identidade envolve o roubo de informações pessoais, tais como números de previdência social ou detalhes de contas bancárias, com a intenção de utilizá-las para fins fraudulentos. Os esquemas de phishing são tentativas fraudulentas de obter informações sensíveis, tais como nomes de usuário e senhas, disfarçando-se de sites ou e-mails legítimos.

O hacking ocorre quando uma pessoa não autorizada ganha acesso a um sistema ou rede de computadores, frequentemente com a intenção de roubar ou modificar dados. Os ataques maliciosos envolvem a instalação de software malicioso em um sistema de computador, muitas vezes enganando os usuários através de esquemas de phishing ou táticas de engenharia social.

Os crimes cibernéticos podem ter consequências graves, desde perda financeira até danos à reputação e até mesmo consequências legais. É importante que indivíduos e empresas tomem medidas proativas para se protegerem contra essas ameaças e para denunciarem quaisquer incidentes às autoridades competentes. Permanecendo conscientes destes riscos e tomando as medidas necessárias. Neste viés, Araújo Lima (1995, p. 127 e 133) consigna que:

> No atual estágio de desenvolvimento científico, o conceito de criminalidade informática deverá girar em torno da ideia de direito de informação e de direito de informática, nos quais a informação, o ambiente e a relevância econômica serão fatores fundamentais. A informação há de ser considerada como um bem de valor econômico, cultural, e político, além de se haver transformado num potencial de risco específico. O ambiente há de ser tratado como um elemento gerador da confiabilidade e segurança da informação, a despeito de sua vulnerabilidade. Esse novo modo dever as coisas, torna evidente que os bens intangíveis devem ser tratados de forma inteiramente diferente daquela pela qual são tratados os crimes tradicionais, de caráter material (LIMA, 1995).

É importante notar que o crime cibernético é um campo em constante evolução, com novas táticas e ferramentas sendo desenvolvidas o tempo todo, por isso é crucial que indivíduos e organizações se mantenham atualizados sobre as últimas ameaças e medidas de segurança. Conheço por criminalidade informática o recente fenômeno histórico-sociocultural caracterizado pela elevada incidência de ilícitos penais (delitos, crimes e contravenções) que têm por objeto material ou meio de execução o objeto tecnológico informático (hardware, software, redes, etc.). (FELICIANO, 2000, p.42)

Os crimes cibernéticos puros, segundo COSTA (1997, p.03) seriam toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas.

Outro aspecto chave na discussão do cibercrime é o impacto que ele pode ter sobre os indivíduos e a sociedade como um todo. O cibercrime pode levar a perdas financeiras, danos à reputação pessoal e profissional, e até mesmo danos físicos em casos extremos. Também pode ter consequências de longo alcance em uma escala mais ampla, incluindo danos à infraestrutura crítica, à segurança nacional e à economia.

Finalmente, podemos falar sobre as formas como o crime cibernético é abordado e prevenido. Isto inclui esforços das agências de aplicação da lei, regulamentações governamentais e iniciativas do setor privado, bem como campanhas de educação e conscientização para ajudar indivíduos e organizações a se protegerem de ameaças cibernéticas. O cibercrime representa uma séria ameaça à nossa sociedade moderna. Com o aumento da tecnologia digital, o número de ataques cibernéticos aumentou exponencialmente, causando perdas financeiras significativas e violações de dados pessoais. Assim, é essencial falar sobre os crimes cibernéticos e educar as pessoas sobre este assunto.

Para prevenir o crime cibernético, indivíduos e organizações precisam estar vigilantes e adotar uma abordagem multicamadas para a segurança cibernética. Isto inclui a implementação de senhas fortes, atualização regular de software, uso de software antivírus e backup de dados importantes. Além disso, as pessoas devem ser cuidadosas ao compartilhar informações pessoais on-line, e devem evitar clicar em links suspeitos ou fazer o download de anexos não solicitados.

3. DELITOS COMETIDOS ATRAVÉS DA INTERNET

A origem do crime digital remonta à década de 1970, quando especialistas em tecnologia da informação passaram a buscar formas de burlar os sistemas de segurança, com foco especial nas instituições financeiras. Na atualidade, a mentalidade e os métodos dos cibercriminosos mudaram significativamente. A principal transformação é que hoje qualquer pessoa com acesso à internet — independentemente do nível técnico — pode cometer infrações digitais, utilizando o computador como ferramenta principal (CASTRO, 2003). Assim, até usuários domésticos podem se envolver, ativa ou passivamente, em litígios relacionados ao cibercrime.

Os primeiros registros de delitos digitais surgiram nos anos 70, sendo executados majoritariamente por profissionais altamente especializados em informática, que tinham como principal objetivo violar os sistemas de segurança de grandes corporações, sobretudo instituições bancárias. Com o tempo, o perfil do infrator evoluiu: atualmente, basta ter acesso à internet e conhecimentos básicos para cometer um crime virtual com sucesso (CARVALHO, 2020, p. 9).

No ambiente digital, garantias fundamentais previstas na Constituição Federal — como o direito à privacidade, à igualdade e à dignidade — têm sido frequentemente violadas. Muitas vezes, essas ações não eram nem sequer classificadas como crime, escapando assim do alcance penal. Criminosos digitais exploram as brechas existentes na legislação para continuar praticando condutas ilícitas que impactam negativamente desde cidadãos comuns até empresas de diferentes portes, incluindo o próprio Estado, que já sofreu prejuízos significativos com ataques a seus sistemas de informação (CARVALHO, 2020).

Essas ações são conhecidas por diversos nomes: crimes cibernéticos, fraudes digitais, delitos informáticos, crimes eletrônicos, entre outras denominações. A variedade de termos reflete a complexidade e a constante transformação do universo digital.

De acordo com reportagens da CNN e do G1, na madrugada do dia 10 de janeiro, o site oficial do Ministério da Saúde foi alvo de um ataque hacker. A mensagem deixada no portal indicava que dados internos haviam sido copiados e deletados. Outros sistemas ligados à pasta, como o ConecteSUS e o Portal Covid, também foram comprometidos, ficando indisponíveis para acesso.

O meio digital abriga múltiplas formas de delitos, e ainda não há consenso sobre a melhor nomenclatura para classificá-los. Termos como “crime digital”, “fraude cibernética” e “abuso de sistemas” são utilizados de maneira intercambiável, o que indica que o vocabulário jurídico ainda não conseguiu abranger todas as nuances dessa realidade (POPPER, 2018, p. 48).

A avaliação se uma conduta é criminosa segue uma ordem lógica: primeiro se analisa se o comportamento se enquadra como típico; depois, verifica-se sua ilicitude; por fim, a culpabilidade. Essa estrutura se aplica tanto aos crimes convencionais quanto aos virtuais, pois, em ambos os casos, o comportamento humano pode causar danos relevantes e está sujeito a punição legal (GROSSI, 2005).

O crime digital ultrapassa fronteiras, podendo ser praticado em qualquer parte do mundo. Apesar de ocorrer em um ambiente virtual, seus efeitos e consequências são reais

e similares aos de crimes praticados fora da internet. O autor de um ato que seja típico, ilícito e culpável, mesmo que cometido virtualmente, responde da mesma forma que em casos físicos (BORRI, 2021; CRESPO, 2011).

De forma geral, os cibercriminosos são frequentemente jovens da era digital. Contudo, qualquer indivíduo com algum grau de conhecimento em informática e acesso à internet pode tornar-se autor de delitos com grande potencial destrutivo (GROSSI, 2005).

Os infratores no ambiente virtual podem ser tanto indivíduos altamente especializados, como hackers e crackers, quanto usuários comuns que cometem crimes digitais sem conhecimento técnico avançado. Portanto, não é possível traçar um único perfil do criminoso digital (CARVALHO, 2020).

Segundo Borri (2021), para responsabilizar alguém criminalmente, o Direito Penal precisa se basear em sujeitos concretos — não meras entidades virtuais ou abstratas.
Os crimes cibernéticos envolvem o uso de computadores, redes ou dispositivos conectados para a prática de atividades ilícitas. Embora nem todos os crimes digitais sejam cometidos com o objetivo de lucro, muitos deles são executados por hackers ou cibercriminosos em busca de ganhos financeiros ilícitos (PINHEIRO, 2020).

Os crimes digitais mais comuns englobam diversas práticas, como a interceptação indevida de dados confidenciais de indivíduos ou organizações, o furto de informações bancárias e financeiras, e a invasão de sistemas computacionais, sejam eles pessoais, corporativos ou parte de redes complexas (POPPER, 2018).

As ações ilícitas praticadas no ambiente virtual são classificadas como cibercrimes e se caracterizam por serem condutas típicas, antijurídicas e culpáveis, cometidas através da internet. Esses atos podem resultar em violação de sigilo, danos patrimoniais e fraudes, como o estelionato digital. Apesar da gravidade, muitas dessas infrações ainda carecem de regulamentações penais adequadas, o que favorece a atuação impune de hackers e crackers (POPPER, 2018).

Dentro da tipologia dos crimes cibernéticos, existe uma distinção entre os chamados delitos próprios e os impróprios. Os delitos próprios ocorrem quando o agente utiliza diretamente o sistema informático da vítima, fazendo do computador tanto o meio quanto o alvo da ação criminosa. Exemplos incluem invasões não autorizadas (hacking), disseminação de malwares e obstrução do funcionamento de sistemas (PINHEIRO, 2020; POPPER, 2018).

Por outro lado, os crimes digitais impróprios são aqueles em que o computador serve apenas como uma ferramenta para realizar atos ilegais que atingem bens jurídicos protegidos, como a honra, o patrimônio ou a intimidade de terceiros (POPPER, 2018). Nesse caso, o dispositivo é o meio, mas não o alvo central do delito.

Diante do crescimento exponencial dessas práticas, o Brasil implementou medidas legislativas específicas para combater os crimes eletrônicos. A Lei nº 12.737, de 2012, conhecida como "Lei Carolina Dieckmann", foi um marco na tipificação de crimes digitais, estabelecendo punições para invasões de sistemas, roubo de dados e interrupção de serviços online. Além disso, novos projetos em tramitação no Senado propõem penas mais severas para infrações cometidas no ambiente virtual (RIBEIRO, 2019).

A segurança cibernética, por sua vez, deve ser compreendida como a proteção das conexões digitais e dos sistemas interligados por meio de redes de telecomunicação. Esse conceito abrange não apenas os dados, mas também os dispositivos e objetos conectados, que podem ser controlados remotamente ou utilizados em processos automatizados dentro do chamado ciberespaço (SILVA, 2020).

Nesse contexto, o Código Penal passou a incorporar o crime de "Invasão de Dispositivo Informático" por meio do Artigo 154-A. A norma descreve como criminosa a conduta de invadir, sem autorização, dispositivos alheios — conectados ou não à internet — com o intuito de acessar, modificar ou eliminar dados, ou ainda instalar vulnerabilidades que possibilitem obter vantagem ilícita. A pena básica prevista é de detenção de três meses a um ano, além de multa. Em casos agravados, há previsão de aumento de pena (SOUZA, 2020).

A criação dessa legislação representa um avanço no ordenamento jurídico brasileiro, refletindo a crescente preocupação da sociedade com a privacidade e a segurança de suas informações no meio digital. A tipificação específica da invasão de sistemas como crime demonstra o esforço em proteger dados pessoais e profissionais, reconhecendo a importância do sigilo digital como um direito fundamental (SILVA, 2020; SOUZA, 2020).

4. PERFIL DO CRIMINOSO

O cibercriminoso não possui um perfil definido, tampouco exibe traços específicos que permitam identificá-lo facilmente no ambiente digital. A ausência de características uniformes dificulta distinguir quem representa uma ameaça no mundo virtual.

Para realizar certos atos ilícitos online, não é indispensável ter domínio técnico avançado em informática. Exemplos disso são comentários ofensivos de cunho racista

feitos nas redes sociais. Essas manifestações discriminatórias não exigem conhecimento especializado, apenas a intenção de ferir ou humilhar pessoas por pertencerem a grupos étnicos considerados, erroneamente, inferiores.

Independentemente do grau de familiaridade com a tecnologia, qualquer pessoa está apta a cometer infrações digitais, sejam elas de grande ou pequena escala. Assim, torna-se impossível traçar um padrão fixo do autor dessas práticas.

O termo "hacker" costuma evocar a imagem de um especialista em tecnologia que utiliza seu conhecimento para atividades ilegais, como invasões de sistemas, roubo de senhas e extração de dados. No entanto, essa percepção não abrange a totalidade do que significa ser hacker.

Existe uma categoria de hackers conhecida como "white hats" ou hackers éticos, que são contratados por empresas justamente para testar a segurança de seus próprios sistemas. Esses profissionais identificam vulnerabilidades e sugerem melhorias, atuando como verdadeiros aliados da cibersegurança.

Esses especialistas têm como objetivo conhecer, explorar e aprimorar sistemas, redes e equipamentos de forma construtiva. Seu trabalho está pautado na prevenção de ataques e na solução de falhas, garantindo maior proteção aos dados.

Na contramão dos white hats estão os crackers, termo que surgiu por volta de 1985 para diferenciar os que usam o conhecimento tecnológico com finalidades criminosas. Os crackers invadem sistemas, modificam programas, violam aplicativos e agem em busca de lucro ilícito. É comum associá-los à pirataria digital.

Além deles, existem outros grupos menos conhecidos, como os phreakers, especializados em fraudar sistemas de telefonia e sinal de televisão, e os carders, que praticam fraudes com cartões de crédito, roubando dados para realizar compras indevidas ou saques em nome das vítimas.

Sérgio Marcos Roque (2007, p. 25) define o crime informático como qualquer conduta prevista em lei como criminosa, na qual o computador é empregado como ferramenta para a prática do delito ou figura como alvo direto da ação.

De forma mais detalhada, Fabrizio Rosa (2002, p. 53-54) conceitua esses crimes como ações que comprometem a integridade dos dados e recursos de sistemas computacionais, afetando processos de armazenamento, processamento ou transmissão de informações. Os crimes de informática, segundo ele, envolvem dois elementos inseparáveis: os dados — que são objeto do ataque — e o próprio sistema computacional — que serve de meio para a execução do ato. Esses delitos podem atingir uma ampla gama

de bens jurídicos, desde a economia e o patrimônio, até a privacidade, a honra, a liberdade e até a integridade de pessoas e instituições públicas ou privadas.

Hoje, os estudiosos dividem os crimes digitais principalmente em duas categorias: crimes próprios e crimes impróprios. Nos crimes cibernéticos próprios, o computador é um elemento indispensável à execução do delito — ou seja, sem ele o crime não ocorre. Nestes casos, os dados digitais são o bem jurídico diretamente lesado, como ocorre em ataques a sistemas de dados e invasões em redes protegidas.

Por sua vez, os crimes cibernéticos impróprios são aqueles em que o computador é utilizado apenas como meio para se alcançar outro objetivo ilícito, como, por exemplo, aplicar golpes financeiros ou disseminar informações falsas, onde o foco não está na máquina em si, mas sim nas consequências causadas pela ação.

Os crimes virtuais classificados como impróprios não exigem, necessariamente, o uso direto de um computador para gerar consequências no mundo real. Seus efeitos vão além do ambiente digital e podem atingir a esfera física, como ocorre em casos de calúnia, difamação, injúria, entre outros. Esses delitos podem ser praticados tanto por usuários comuns quanto por indivíduos com maior domínio tecnológico. Enquanto alguns crimes exigem técnicas mais sofisticadas, como o roubo de dados por agentes maliciosos, outros, como o ciberbullying ou os crimes contra a honra, podem ser cometidos por qualquer pessoa, mesmo com pouco conhecimento técnico. Entre os métodos mais comuns utilizados pelos cibercriminosos estão o phishing, o trojan e a engenharia social.

O phishing é uma das formas de fraude mais antigas e disseminadas na internet. Ele se baseia na manipulação psicológica das vítimas por meio de mensagens que imitam comunicações legítimas de instituições conhecidas, como bancos ou lojas online. O objetivo é convencer o usuário a fornecer informações pessoais, senhas ou dados bancários. O criminoso “lança a isca” com um link atraente, enviado por e-mail, SMS ou redes sociais, e, ao clicar, a vítima é induzida a preencher formulários falsos ou a realizar pagamentos, transferindo seus dados ou dinheiro diretamente para o golpista. O nome "phishing" é uma alusão à prática de pescar, em que a isca é utilizada para atrair a vítima no vasto “oceano” da internet.

Já o trojan, ou cavalo de Troia, recebe esse nome em referência à lenda grega. Trata-se de um software malicioso que se disfarça como um programa legítimo, enganando o usuário ao ser executado. Ao ser instalado, abre brechas no sistema da vítima, permitindo o acesso remoto por criminosos. Diferente de outros vírus, o trojan é autônomo e não precisa infectar outros arquivos para funcionar, o que o torna mais difícil de ser detectado.

A prevenção consiste, principalmente, em evitar instalar arquivos de fontes desconhecidas e manter sistemas de segurança atualizados.

A engenharia social, por sua vez, é um método que antecede a era digital, mas que se adaptou perfeitamente ao ambiente virtual. Nessa prática, o golpista manipula psicologicamente a vítima para obter informações confidenciais, muitas vezes se passando por profissionais de confiança, como técnicos, médicos ou representantes de instituições. Antes mesmo da popularização da internet, já existiam casos de criminosos que invadiam empresas com disfarces para coletar dados ou roubar valores. Atualmente, esse tipo de golpe é comumente associado a mensagens falsas, e-mails suspeitos ou ligações fraudulentas, em que erros gramaticais ou informações incoerentes podem ser indicativos da fraude.

Outra forma recorrente de crime virtual é o cyberbullying, que consiste em agressões praticadas no ambiente digital. A palavra é a junção dos termos ingleses "cyber" (virtual) e "bullying" (intimidação). Essa prática se caracteriza por ofensas repetidas, humilhações e hostilidade intencional com o uso das tecnologias de informação e comunicação. Diferente do bullying presencial, o cyberbullying tem um impacto potencialmente mais grave, pois os ataques podem atingir proporções globais e as informações compartilhadas dificilmente podem ser apagadas da internet. Isso torna a vítima exposta a constrangimentos constantes, sem controle sobre a circulação dos conteúdos.

As formas mais comuns de cyberbullying incluem o vazamento de imagens íntimas ou montagens constrangedoras, a disseminação de pornografia infantil e críticas ofensivas à aparência física. Muitos agressores se sentem protegidos pelo aparente anonimato proporcionado pela internet, acreditando que, por estarem por trás de perfis falsos, estão imunes às consequências. Essa falsa sensação de impunidade estimula comportamentos que, fora do ambiente virtual, dificilmente seriam manifestados.

O chamado “hater” é um exemplo típico de agressor virtual. Esse termo é utilizado para designar usuários que espalham ódio nas redes sociais, atacando outras pessoas com insultos e provocações. O crescimento das redes sociais e o fácil acesso à internet fizeram com que essas atitudes se tornassem cada vez mais comuns, variando de simples comentários maldosos a ataques organizados e sistemáticos.

Apesar do caráter virtual, o cyberbullying é um crime previsto na legislação brasileira. A prática pode ser enquadrada em diversos artigos do Código Penal, como o artigo 138 (calúnia), artigo 140 (injúria, incluindo injúria racial), artigo 139 (difamação) e artigo 218-C, que trata do vazamento de conteúdo íntimo sem consentimento. As penas para esses

crimes podem chegar a até quatro anos de reclusão, além da obrigação de indenizar a vítima por danos morais. Dessa forma, a legislação busca responsabilizar os agressores e oferecer meios de proteção às vítimas no ambiente digital.

5. INSUFICIÊNCIA DE PUNIÇÕES E DESAFIOS LEGAIS

A introdução ao tema da ausência de punições em crimes cibernéticos é um assunto de grande relevância nos dias de hoje. Com o avanço da tecnologia, crimes virtuais têm se tornado cada vez mais comuns e sofisticados, porém, muitas vezes, os criminosos não são identificados e, consequentemente, não recebem punições adequadas pelo que fizeram. Isso faz com que haja uma sensação de impunidade e abre brechas para a continuação desses delitos. Nesse contexto, é imprescindível debater meios eficazes para identificar e punir os responsáveis por crimes cibernéticos, garantindo segurança para a sociedade como um todo.

Atualmente, com o avanço da tecnologia, os crimes virtuais e cibernéticos se tornaram comuns. Para prevenir e combatê-los, medidas são necessárias. Em primeiro lugar, é crucial que a população seja educada sobre os riscos e perigos da internet, e como se proteger. Além disso, as empresas devem investir em medidas de segurança cibernética para evitar ataques e vulnerabilidades em seus sistemas. As autoridades também precisam intensificar a fiscalização e punir os criminosos virtuais, promovendo uma campanha de conscientização sobre a importância de denunciar esse tipo de crime. Só assim, poderemos garantir a segurança dos nossos dados e informações na internet.

A insuficiência de punição nos crimes virtuais vem se tornando um problema cada vez mais relevante em nossa sociedade digital. Com o crescimento exponencial do uso da internet, redes sociais e dispositivos móveis, crimes cibernéticos como cyberbullying, fraudes online, hacking, phishing, entre outros, têm se tornado cada vez mais comuns. No entanto, apesar da gravidade desses crimes, muitas vezes a punição não é adequada ou suficiente para coibir sua ocorrência. Isso ocorre porque muitos países ainda não possuem legislação específica para crimes virtuais ou porque a legislação existente não é efetivamente aplicada. Cassanti (2014, p. 175) entende que “as forças policiais no Brasil não estão estruturadas e treinadas adequadamente para enfrentar, com eficiência, os crimes virtuais. Pelo contrário, alguns estados estão extinguindo os serviços que possuem”

Além disso, há a dificuldade em identificar e rastrear os criminosos virtuais, que muitas vezes usam tecnologias avançadas e se utilizam de falsas identidades para cometer.

Apesar dos esforços empenhados no combate aos crimes virtuais, a criminalidade

> informática, usufruindo das novas tecnologias que surgem a cada momento, desafia os profissionais da área, no sentido de que estes ainda não estão totalmente preparados para enfrentar esse tipo de crime em decorrência de suas características que acabam por dificultar a investigação criminal. (DIAS, 2017, p. 33)

Com o aumento da dependência da tecnologia e da internet, os crimes cibernéticos estão se tornando cada vez mais frequentes e sofisticados, e muitas vezes as leis atuais não são suficientes para proteger as vítimas e punir os criminosos. Um dos principais desafios enfrentados pelas autoridades é lidar com a natureza internacional das atividades criminosas na internet. Muitos criminosos cibernéticos podem estar localizados em países diferentes das vítimas e usar técnicas de ocultação de identidade para evitar a detecção e a punição.

Pincerati (2018, p.45) discorre que “o Brasil ainda não possui uma linha de planejamento efetiva para acompanhar tais evoluções, acabando por prejudicar as investigações de vários crimes em virtude da falta de instrumentos ou até mesmo pessoas capacitadas para atuar nessas áreas”

Uma das questões que mais gera polêmica e debates é a falta de punições adequadas para crimes e infrações cometidos. Muitas pessoas acreditam que as leis devem ser mais rígidas e que as penas devem ser mais severas, como forma de inibir a prática de delitos. Porém, há também uma parcela da população que argumenta que essa não é a solução, e que é preciso investir em políticas de prevenção e educação, oferecendo oportunidades para as pessoas que estão em situação de vulnerabilidade social. A discussão sobre a falta de punições adequadas é um tema complexo e requer uma reflexão sobre diferentes perspectivas e soluções possíveis. O inquérito tem um papel de suma importância para a apuração dos crimes virtuais, e através dele que todos os procedimentos investigativos serão realizados a fim de constatar os eventuais criminosos, e futuramente poderá ser utilizado em uma eventual ação penal. (PINCERATI, 2018, p.26)

Muitas pessoas acreditam que a falta de punições severas para os criminosos cibernéticos é devido à dificuldade em rastrear e provar suas atividades ilegais por meios tradicionais de investigação. As leis cibernéticas variam de país para país, e em algumas jurisdições, as autoridades competentes não têm as capacidades técnicas para lidar com crimes cibernéticos. Dias (2017, p. 33) aduz que “percebe-se que a investigação de crimes digitais apresenta diversos desafios, destacando-se a necessidade de investimento em recursos tecnológicos e em recursos humanos como um dos aspectos mais relevantes.”

Os provedores não são obrigados a guardar os registros de acesso quando um

determinado indivíduo acessa a Internet. Isso dificulta bastante a persecução penal na busca da infração em crimes por computador, notadamente na Internet. Exemplo de situações em que isso ocorre são os computadores utilizados em *lan houses, cybers-café* ou salas públicas de serviços de Internet, as quais não se têm controle algum sobre quem usa o computador ou com que finalidade o utiliza. (MEDEIROS, 2010, p.5)

No Brasil, A “Lei Carolina Dieckmann” acrescentou ao Código Penal os artigos 154-A e 154-B. Porém, em 27 de maio de 2021, o artigo 154-A foi alterado pela Lei nº 14.155, que modificou o próprio tipo penal desse referido artigo. O artigo 154-A ficou com a seguinte redação:

> “Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021) Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021) § 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. (Incluído pela Lei nº 12.737, de 2012) Vigência § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. (Redação dada pela Lei nº 14.155, de 2021) § 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: (Incluído pela Lei nº 12.737, de 2012) Vigência Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021) § 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. (Incluído pela Lei nº 12.737, de 2012) Vigência § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012) I - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012) Vigência II - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012) Vigência III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou (Incluído pela Lei nº 12.737, de 2012) Vigência IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº 12.737, de 2012)” (Brasil, online, 2021).

Um dos maiores desafios legais enfrentados pela sociedade é a implementação de leis de punição para crimes cibernéticos. Com o aumento constante das atividades criminosas na internet, torna-se necessário que haja uma regulamentação específica para essas questões. No entanto, a complexidade do ambiente virtual, a falta de cooperação entre os países e a dificuldade em identificar os responsáveis pelos crimes dificultam a criação de leis eficientes. Além disso, a própria natureza cibernética dos delitos pode gerar divergências conceituais, exigindo que as leis sejam constantemente atualizadas e adaptadas. Diante desse contexto, é imprescindível que os governos e organizações colaborativas atuem em conjunto. “A lei do Marco Civil foi criada para suprir as lacunas no

sistema jurídico em relação aos crimes virtuais, num primeiro momento tratando dos fundamentos, conceitos para sua interpretação e objetivos que o norteiam, além de enumerar os direitos dos usuários, tratar de assunto polêmicos como por exemplo a solicitação de histórico de registros, a atuação do poder público perante os crimes virtuais e por último garante o exercício do direito do cidadão de usufruir da internet de modo individual e coletivo estando devidamente protegido.” (OLIVEIRA, et. al., 2017, p. 126).

A ausência de punição para crimes cibernéticos pode trazer diversas consequências graves. Primeiramente, cria um ambiente propício para o aumento da ocorrência de delitos cibernéticos, já que os criminosos se sentem impunes e sem medo de serem pegos. Isso pode levar a um aumento significativo de fraudes, invasões de privacidade, extorsões, entre outros crimes.

Além do mais, a falta de punição pode minar a confiança nas plataformas digitais. Quando os usuários percebem que não há consequências para os crimes cometidos no ambiente virtual, eles se tornam mais cautelosos e inseguros em relação à segurança de suas informações pessoais. Isso pode prejudicar o crescimento e desenvolvimento do comércio eletrônico, por exemplo, que depende da confiança dos consumidores. “Embora a necessidade de ordem judicial surja como um ato para inibir o abuso por parte de autoridades, dentro da investigação de crimes cibernéticos acaba por criar serias barreiras para investigação” (PINCERATI 2018, p.48).

Todas as informações obtidas dos provedores passam a ser analisadas pelos agentes de polícia, descartando informações desnecessárias que não irão contribuir com a investigação. E eventualmente formalizando as provas necessárias a investigação. Neste ponto vale salientar que a uma grande dificuldade na maioria das vezes, pois atualmente muitos usuários e inclusive criminosos acabam por ocultar sua navegação dificultando assim a localização do usuário. (PINCERATI, 2018, p.30)

As leis e políticas de proteção cibernética são essenciais na prevenção de crimes e garantia de punição para os responsáveis. No mundo digital, é comum que ocorram violações de dados pessoais, fraudes eletrônicas e outros tipos de delitos. Por isso, é importante que o Estado elabore leis que regulamentem o uso do computador e da internet, além de promover ações para conscientização da população sobre a segurança na rede. Dessa forma, é possível criar um ambiente mais seguro para as pessoas, reduzindo o número de crimes cibernéticos e garantindo que os responsáveis sejam punidos de acordo com a legislação vigente.

O problema da legislação que normatiza o “novo” é que muitas vezes resultam na

criação de leis vagas e esparsas, que não alcançam de maneira eficaz a evolução da sociedade, visto que os crimes têm se tornado cada vez menos óbvios, sendo difícil prever todas as possibilidades. (PAGNOZZI, 2018, p.38)

7. CONSIDERAÇÕES FINAIS

Ao longo deste estudo, foi possível compreender que os crimes cibernéticos configuram uma das mais complexas e desafiadoras formas de criminalidade contemporânea, especialmente diante do constante avanço tecnológico e da ampla utilização da internet em diversas esferas da sociedade. A pesquisa revelou que, embora a legislação brasileira tenha evoluído nos últimos anos, ainda enfrenta dificuldades significativas para acompanhar a rapidez das transformações digitais, o que acaba por comprometer a eficácia na prevenção e punição desses delitos.

Além disso, a análise dos diferentes tipos de crimes cometidos pela internet evidenciou a diversidade e sofisticação das práticas criminosas, que vão desde fraudes simples até ataques cibernéticos organizados, impactando tanto indivíduos quanto instituições públicas e privadas. O perfil do criminoso digital também se mostra complexo e multifacetado, exigindo uma abordagem que considere não apenas aspectos legais, mas também sociais, psicológicos e tecnológicos para melhor compreensão e combate ao problema.

As insuficiências da legislação vigente e as lacunas na aplicação das punições demonstram a necessidade urgente de atualização normativa, capacitação dos profissionais envolvidos na área jurídica e ampliação da cooperação internacional para o enfrentamento eficaz dos crimes cibernéticos. Somente por meio de esforços conjuntos entre órgãos públicos, iniciativa privada e sociedade civil será possível criar um ambiente digital mais seguro e resguardar os direitos dos usuários.

Por fim, este trabalho contribui para o debate sobre a importância de políticas públicas integradas e de uma legislação dinâmica, que possa acompanhar as inovações tecnológicas e assegurar a responsabilização adequada dos infratores. É imprescindível que o tema continue sendo objeto de estudos e discussões, para que o sistema jurídico brasileiro possa evoluir e responder de forma eficaz aos desafios impostos pelo cibercrime na atualidade.

REFERÊNCIAS

ARAÚJO LIMA, Gilberto de. **Informática e direito penal:** novas formas de criminalidade. 2. ed. São Paulo: Saraiva, 1995.

BAUMAN, Zygmunt. **Modernidade líquida.** 1. ed. Rio de Janeiro: Zahar, 2001.

BECK, Ulrich. **Sociedade de risco:** rumo a uma outra modernidade. 2. ed. São Paulo: Editora 34, 2018.

BORRI, Felipe. **Crimes cibernéticos e o Direito Penal brasileiro.** São Paulo: Saraiva, 2021.

CARVALHO, Lílian Mendes de. **Cibercrimes e responsabilidade penal.** 2. ed. Belo Horizonte: Del Rey, 2020.

CASSANTI, João. **Investigação criminal digital:** aspectos práticos e jurídicos. São Paulo: Revista dos Tribunais, 2014.

CASTRO, Rubens de. **Crimes cibernéticos:** aspectos penais. São Paulo: RT, 2003.

COSTA, José de Faria. **Cibercriminalidade:** aspectos jurídicos e criminológicos**.** Coimbra: Almedina, 1997.

CRESPO, Elena. **Crimes informáticos e o sistema jurídico penal.** Lisboa: Quid Juris, 2011.

DIAS, Daniel. **Criminalidade digital:** investigação e prevenção. São Paulo: Atlas, 2017.

DURKHEIM, Émile. **As regras do método sociológico.** São Paulo: Companhia Editora Nacional, 1999.

FELICIANO, Guilherme. **Crimes informáticos:** uma nova fronteira do direito penal. Revista de Direito Penal, São Paulo, n. 3, p. 42-53, 2000.

GROSSI, Adriano. **Responsabilidade penal nos crimes virtuais**. Curitiba: Juruá, 2005.

JESUS, Damásio de; MILAGRE, José Antônio. **Crimes digitais e proteção de dados.** São Paulo: Saraiva, 2006.

MANZUR, Enrique del Río; PINHEIRO, Cícero. **Crimes informáticos:** a nova criminalidade. São Paulo: Revista dos Tribunais, 2000.

MACHADO, Júlio Fabrício. **Sociedade da informação e criminalidade.** São Paulo: Malheiros, 2010.

MEDEIROS, Elizabete. **Internet e Direito Penal:** desafios à persecução penal na era digital. Porto Alegre: Livraria do Advogado, 2010.

OLIVEIRA, Rafael; et al. **Marco Civil da Internet:** comentários à Lei nº 12.965/2014. Rio de Janeiro: Forense, 2017.

PAGNOZZI, Fabiano. **Crimes digitais:** desafios à investigação criminal. São Paulo: Rideel, 2018.

PINCERATI, Leonardo. **Investigação de crimes cibernéticos:** aspectos práticos e jurídicos. São Paulo: Método, 2018.

PINHEIRO, André. **Criminalidade digital e Direito Penal brasileiro.** Salvador: JusPodivm, 2020.

POPPER, Nathaniel. **Crimes digitais e o sistema de justiça criminal.** São Paulo: Atlas, 2018.

RIBEIRO, Bruno. **Direito digital:** fundamentos, legislação e jurisprudência. São Paulo: Saraiva, 2019.

ROQUE, Sérgio Marcos. **Crimes informáticos e direito penal.** Curitiba: Juruá, 2007.

SHOUERI, Luís Eduardo. **Contratos eletrônicos:** segurança e validade jurídica. São Paulo: Revista dos Tribunais, 2001.

SILVA, Lúcio Costa da. **Segurança da informação e crimes digitais.** Brasília: Senado Federal, 2020.

SOUZA, Marcelo Tadeu de. **Crimes informáticos e Lei nº 12.737/2012.** Belo Horizonte: Del Rey, 2020.

SPADINGER, Robert. **Direito e internet:** fundamentos jurídicos para o mundo digital. Porto Alegre: Fabris, 2012.

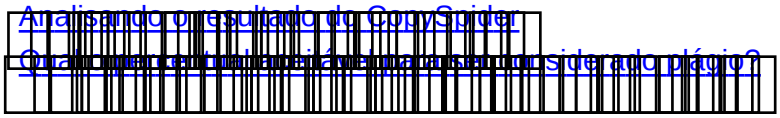
Relatório do Software Anti-plágio CopySpider

Para mais detalhes sobre o CopySpider, acesse:https://copyspider.com.br

Instruções

Este relatório apresenta na próxima página uma tabela na qual cada linha associa o conteúdo do arquivo de entrada com um documento encontrado na internet (para "Busca em arquivos da internet") ou do arquivo de entrada com outro arquivo em seu computador (para "Pesquisa em arquivos locais"). A quantidade de termos comuns representa um fator utilizado no cálculo de similaridade dos arquivos sendo comparados. Quanto maior a quantidade de termos comuns, combinada com o agrupamento desses termos, maior a similaridade entre os arquivos. É importante destacar que a classificação da semelhança como Alta, Moderada e Baixa não representa um "índice de plágio". Por exemplo, documentos que citam de forma direta (transcrição) outros documentos, podem ter uma similaridade Alta e ainda assim não podem ser caracterizados como plágio. Há sempre a necessidade do avaliador fazer uma análise para decidir se as semelhanças encontradas caracterizam ou não o problema de plágio ou mesmo de erro de formatação ou adequação às normas de referências bibliográficas. Para cada par de arquivos, apresenta-se uma comparação dos termos semelhantes, os quais aparecem em vermelho.

Veja também:



Versão do CopySpider: 3.2
Relatório gerado por: alexia.santos@ucsal.edu.br
Análise no modo: Web/Rápida (75.0%) em 22:01
Idioma da busca: Português

Arquivos	Termos comuns	Semelhança	Agrupamento
TCC - LUCAS.pdf	866	Moderada	Alto
X www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/			
TCC - LUCAS.pdf	580	Baixa	Alto
X jus.com.br/artigos/90334/crimes-ciberneticos-era-insu			
TCC - LUCAS.pdf	285	Baixa	Moderado
X www.reavale.br/Comum/midias/0163c982-1f5d-496f-b			
TCC - LUCAS.pdf	275	Baixa	Moderado
X experteditora.com.br/wp-content/uploads/2023/07/Cri			
TCC - LUCAS.pdf	273	Baixa	Moderado
X repositorio.pucrs.br/dspace/bitstream/10923/24954/1/			
TCC - LUCAS.pdf	270	Baixa	Moderado
X revistaft.com.br/area/educacao-dos-crimes-ciberneticos-re			
TCC - LUCAS.pdf	271	Baixa	Baixo
X repositorio.ufms.br/jspui/retrieve/8251405c-ccf8-4906			
TCC - LUCAS.pdf	247	Baixa	Baixo
X www.iosrjournals.org/iosr-jbm/papers/Vol26-issue11/			
TCC - LUCAS.pdf	227	Baixa	Baixo
X core.ac.uk/download/pdf/196147375.pdf			
TCC - LUCAS.pdf	199	Baixa	Baixo
X pt.wikipedia.org/wiki/Hist%C3%B3ria_da_humanidad			

==========

Arquivo 1: TCC - LUCAS.pdf (7112 termos)

Arquivo 2: www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/eventos/cnm-2019/coletaneas-de-artigos/coletanea_de_artigos_principais_sobre_crimes_ciberneticos.pdf (76995 termos)

Termos comuns: 866

Índice de similaridade antigo: 1,04%

Novo índice de similaridade: 12,17%

Índice de agrupamento: Alto

O texto abaixo é o conteúdo do documento **Arquivo 1**. Os termos em vermelho foram encontrados no documento **Arquivo 2**. Id da comparação: 6a1f89a1f318b4bx247

==========

UNIVERSIDADE CATÓLICA DO SALVADOR
FACULDADE DE DIREITO
BACHARELADO DE DIREITO

OS AVANÇOS DOS CRIMES CIBERNÉTICOS E A LACUNA EXISTENTE NA LEGISLAÇÃO BRASILEIRA

LUCAS MACEDO CABRAL

SALVADOR
2025

LUCAS MACEDO CABRAL
OS AVANÇOS DOS CRIMES CIBERNÉTICOS E A LACUNA EXISTENTE NA LEGISLAÇÃO BRASILEIRA

Trabalho de Conclusão de Curso apresentado à Universidade Católica do Salvador, como requisito parcial para a obtenção do Título de Graduado em Direito.

Orientador: Ms. Cristiano Lázaro

SALVADOR
2025

FICHA DE APROVAÇÃO

Trabalho de conclusão de curso aprovado como requisito parcial para obtenção do grau de Bacharel em Direito da Universidade Católica do Salvador.

Lucas Macedo Cabral
Acadêmico

Cristiano Lázaro
Professor Orientador

Salvador,_____ de _____de 2025.

RESUMO

Com o avanço da tecnologia e a popularização da internet, surgiram novas formas de criminalidade no ambiente virtual, conhecidas como crimes cibernéticos. Essas práticas, que afetam indivíduos, empresas e instituições, representam um desafio crescente para o ordenamento jurídico. A escolha do tema se justifica pela frequência e complexidade dos delitos digitais, que muitas vezes não encontram respostas eficazes na legislação atual. Diante disso, o problema central desta pesquisa é: como a legislação brasileira tem enfrentado os crimes cibernéticos e quais são suas

limitações na punição dos infratores? Para responder a essa questão, adota-se como metodologia a revisão bibliográfica, com base em obras jurídicas, artigos científicos e documentos oficiais. O objetivo geral é analisar os desafios legais no combate aos crimes cibernéticos no Brasil. Como objetivos específicos, busca-se: entender os conceitos e a evolução histórica dos crimes digitais; identificar os principais delitos cometidos pela internet; traçar o perfil dos criminosos; e discutir as falhas legais e punitivas. O trabalho está estruturado em quatro capítulos: o primeiro trata dos conceitos e da historicidade dos crimes cibernéticos; o segundo apresenta os principais delitos virtuais; o terceiro analisa o perfil do infrator; e o quarto discute as insuficiências legais e os desafios enfrentados pela Justiça.

Palavras-chave: Crimes Cibernéticos. Internet. Responsabilidade penal.

ABSTRACT

With the advancement of technology and the popularization of the internet, new forms of crime have emerged in the virtual environment, known as cybercrimes. These practices, which affect individuals, companies, and institutions, represent a growing challenge for the legal system. The choice of this topic is justified by the frequency and complexity of digital offenses, which often do not find effective responses in current legislation. Given this, the central problem of this research is: how has Brazilian legislation addressed cybercrimes, and what are its limitations in punishing offenders? To answer this question, a bibliographic review methodology is adopted, based on legal works, scientific articles, and official documents. The general objective is to analyze the legal challenges in combating cybercrimes in Brazil. As specific objectives, the study seeks to understand the concepts and historical evolution of digital crimes; identify the main offenses committed via the internet; profile the criminals involved; and discuss the legal and punitive shortcomings. The work is structured into four chapters: the first addresses the concepts and historicity of cybercrimes; the second presents the main virtual offenses; the third analyzes the offender?s profile; and the fourth discusses the legal insufficiencies and challenges faced by the justice system.

Keywords: Cybercrimes. Internet. Criminal liability.

SUMÁRIO

1 INTRODUÇÃO

Nas últimas décadas, a revolução digital transformou profundamente a forma como as pessoas se comunicam, trabalham, consomem informações e realizam transações comerciais. Com a expansão da internet e o avanço das tecnologias da informação, surgiu um novo espaço social: o ciberespaço. No entanto, juntamente com as inúmeras oportunidades proporcionadas por esse ambiente virtual, emergiram também novos desafios, entre eles os crimes cibernéticos. Essas práticas delituosas, que se utilizam da rede mundial de computadores como meio ou como fim, representam uma ameaça significativa à segurança individual, institucional e até mesmo nacional.

A relevância do tema se justifica pela crescente incidência e sofisticação dos crimes cometidos por meios digitais, que vão desde fraudes financeiras até ataques cibernéticos complexos a infraestruturas críticas. A legislação, por sua vez, tem enfrentado dificuldades para acompanhar a evolução tecnológica e para garantir a responsabilização efetiva dos criminosos. Diante desse cenário, torna-se fundamental compreender a natureza e as im-