doi.org/10.51891/rease.v10i11.17070

CRIMES CIBERNÉTICOS: PANORAMA LEGISLATIVO

CYBER CRIMES: LEGISLATIVE OVERVIEW. MONTEL

Izadora Fonseca Montel[1]
Jaqueline de Kassia Ribeiro de Paiva[2]

RESUMO: Os crimes cibernéticos definem-se pelas práticas ilícitas cometidas por meio de dispositivos conectados à internet, como invasão de sistemas, fraudes eletrônicas, divulgação de dados pessoais e disseminação de fake news. No Brasil, foram promulgadas leis para enfrentar essa nova realidade: a Lei nº 12.737/2012 (Lei Carolina Dieckmann) que criminalizou a invasão de dispositivos informáticos, a Lei nº 12.965/2014, conhecida como o Marco Civil da Internet e estabeleceu princípios para o uso da internet, assegurando a liberdade de expressão e a privacidade dos usuários. Recentemente, a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) trouxe diretrizes sobre o tratamento e proteção de dados pessoais, que em conjunto com a Lei nº 14.155/2021 endureceu as penas para crimes como fraudes digitais e invasões de dispositivos. O presente estudo teve com o objetivo de apresentar a incidência de crimes cibernéticos em seu panorama legislativo no âmbito jurídico brasileiro, utilizou-se como metodologia a pesquisa bibliográfica e documental de cunho qualitativo que incluiu artigos científicos, relatórios governamentais tal qual a própria legislação vigente acerca do tema, livros e documentos acadêmicos, que datam desde 1990 a 2024, que ao conceituar a tipificar os crimes cibernéticos no âmbito nacional através das principais legislações que versam este tema, pode compreender a necessidade de medidas mais assertivas e leis mais rígidas quanto à prática destes crimes para que assim haja a efetiva interrupção da sua ocorrência.

Palavras-chave: Crimes Cibernéticos. Internet. Direito Digital. Legislação. Tecnologia.

ABSTRACT: Cybercrimes are defined by illicit practices committed through devices connected to the internet, such as system invasions, electronic fraud, disclosure of personal data and dissemination of fake news. In Brazil, important laws were enacted to face this new reality, namely Law nº 12,737/2012 (Carolina Dieckmann Law) which criminalized the invasion of computer devices, Law nº 12,965/2014, known as the Civil Rights Framework for the Internet, established principles for the use of the internet, ensuring freedom of expression and user privacy. Recently, the General Data Protection Law (LGPD – Law nº 13,709/2018) brought guidelines on the processing and protection of personal data, which together with Law nº 14,155/2021 toughened the penalties for crimes such as digital fraud and hacking. devices. In this sense, the present study aimed to present the incidence of cybercrimes in its legislative panorama in the Brazilian legal context, which used bibliographical and documentary research of a qualitative nature as a methodology that included important scientific articles, government reports such as what is the current legislation on the topic, books and academic documents, dating from 1990 to 2024, which, when conceptualizing and classifying cybercrimes at the national level through the main legislation that deals with this topic, can understand the need for more assertive and stricter laws regarding the practice of these crimes so that their occurrence can be effectively interrupted.

Keywords: Cyber Crimes. Internet. Digital Law. Legislation. Technology.

[1] Acadêmica do curso de direito, UNIRG.
[2] Professora orientadora do curso de direito, UNIRG.

INTRODUÇÃO

Com todos os benefícios que o avanço tecnológico pode oferecer, o mal uso da tecnologia levou desafios significativos na forma de crimes cibernéticos. A crescente expansão das relações sociais, econômicas e culturais trouxe vários benefícios, mas também criou espaço para o surgimento de práticas ilícitas que não tão somente adoecem o ambiente digital, como violam o direito de seus usuários.

Neste sentido, POMPEU (2022, p. 14) discorre que "São óbvios os benefícios que o crescimento da tecnologia trouxe tanto para os Governos como para a população, mas, em contrapartida, não se pode olvidar que esse meio de acesso volátil propiciou o aumento do surgimento de vários tipos de crimes." (POMPEU, 2022, p. 14)

Apesar de ser novidade no âmbito tecnológico, esses crimes, que envolvem a prática de atos ilícitos por meio de dispositivos conectados à internet, tem se mostrado abrangente na sua modalidade, desde fraudes financeiras até a disseminação de notícias falsas e o roubo de dados pessoais. Sua natureza complexa e transnacional representa um desafio significativo para os sistemas jurídicos e de segurança em todo o mundo, sentido em que BARBAGALO (2022, p. 02) introduz que "A cibercriminalidade é uma realidade relativamente recente, decorrência da globalização, do aumento exponencial do uso da informática, da evolução das linguagens de programação e do fluxo de dados realizado através da rede mundial de computadores: a internet."

Diante dessa nova realidade que permeia a sociedade brasileira, com o alto uso da tecnologia na vida cotidiana, a facilidade que ela traz e a incidência de crimes cibernéticos, impulsionou o sistema jurídico-legislativo a adaptar-se a esta realidade que não apenas se transforma como se renova rotineiramente.

Assim, POMPEU (2022, p. 12), pontua:

> Com o grande avanço da internet, o qual trouxe uma enorme transformação mundial, e que tem sido a ferramenta essencial para que ocorram todos esses crimes. A internet hoje é reconhecida como uma excelente biblioteca virtual, ferramenta de compra, divulgação de obras pessoais e importante fonte de informações, as possibilidades de sua aplicação são infinitas. Devido ao seu alcance e amplitude, o emprego, necessariamente, regulamentado por lei, em nosso sistema jurídico faz parte da nossa sociedade. No Brasil, essa lei é chamada de Marco Civil. A Internet é crucial para a correta interpretação e aplicação de seus termos pelas autoridades judiciárias." (POMPEU, 2022, p. 12)

Esclarece-se que a evolução legislativa para enfrentar essas novas ameaças teve início com marcos legais específicos, como a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e o Marco Civil da Internet (Lei nº 12.965/2014), que estabelecem direitos e responsabilidades no ambiente

digital. Posteriormente, a Lei Geral de Proteção de Dados (LGPD) e a Lei nº 14.155/2021 ampliaram o escopo de proteção ao tratar de segurança digital e aumentar as probabilidades para crimes virtuais.

Há que se considerar ainda que, os crimes cibernéticos são uma adaptação de crimes já preexistentes no ordenamento jurídico, mas que migraram para o ambiente digital adaptando-se às tecnologias inovadoras que utilizamos no cotidiano, SILVA (2023, p. 07- 08) expõe:

> Portanto, os crimes cibernéticos podem ser compreendidos como eventos que se enquadram como fatos típicos e antijurídicos, perpetrados por meio da internet ou direcionados contra sistemas, dispositivos informáticos e redes de computadores. Essas atividades delituosas são muitas vezes impulsionadas pelas inovações tecnológicas e digitais que surgiram com o propósito de simplificar a vida cotidiana das pessoas. Consequentemente, as facilidades oferecidas, como a capacidade instantânea de realizar postagens, compartilhar fotos, contatos, documentos, vídeos e informações bancárias, tornam-se um terreno fértil para a prática desses crimes, considerando que os criminosos se beneficiam do anonimato, dificultando a identificação pessoal e sua localização. Contudo, além de regulamentar a repressão aos crimes cibernéticos, o legislador enfrentou o desafio de conciliar o combate às infrações com a proteção de direitos fundamentais, como a liberdade de expressão e a privacidade. A discussão sobre o equilíbrio entre a repressão de condutas ilícitas e a preservação de garantias individuais, sobretudo em tempos de desinformação e discurso de ódio, é um dos pontos centrais do debate jurídico atual. (SILVA, 2023, p. 07 – 08)

Assim, o presente trabalho visa apresentar sob o viés do panorama legislativo os crimes cibernéticos que tanto ocorrem no Brasil, visando expender acerca dos seus conceitos, tipificações, bem como o desenvolvimento da legislação brasileira acerca deste tema e discorrer sobre o Caso Carolina Dieckmann, que teve grande impacto no sistema legislativo brasileiro.

1 O PRINCÍPIO DA ERA DIGITAL

No campo acadêmico, o estudo da era digital tem se mostrado essencial para compreender os impactos dessa transformação na estruturação de direitos, na inovação tecnológica e na interação global, logo é importante explorar o significado e as implicações do princípio da era digital, enfatizando sua relevância como pilar norteador de transformações nos mais variados campos do conhecimento e setores da sociedade.

A era digital se transformou profundamente na forma como nos comunicamos, consumimos, ganhamos e interagimos, inaugurando um novo paradigma em todas as esferas da sociedade. Esse aspecto impulsionou o surgimento de um conjunto de valores e normas que orientam o uso ético e sustentável das tecnologias digitais, conhecido como princípio da era digital. Essas diretrizes são fundamentais para garantir que a tecnologia atenda ao bem comum,

promovendo inclusão, privacidade e responsabilidade. Assim, DE OLIVEIRA (2017, p. 121) relembra:

> Uma das primeiras noções de internet surgiu no ano de 1960 através de um projeto elaborado pelo governo americano da época, denominado de ARPANET (Agência de Pesquisa Avançada e Rede), criado só para o uso de militares, a fim de que os mesmos pudessem trocar informações, que era de extrema importância em casos de guerra. No entanto ficou conhecida como internet bem mais tarde, quando a ARPANET passou a ser utilizadas nas universidades dos EUA, e desde então, foi evoluindo constantemente até hoje, trazendo mais facilidades e oportunidades para o nosso cotidiano, além de propiciar para o internauta uma infinidade de informações e momentos até mesmo de lazer." (DE OLIVEIRA, 2017, p. 121)

O primeiro aspecto essencial do princípio da era digital é a inclusão digital e o acesso universal à tecnologia. A conectividade tornou-se indispensável para o exercício de direitos fundamentais, como educação e trabalho. No entanto, existe uma desigualdade de acesso criada o chamado fosso digital, que pode acentuar desigualdades socioeconómicas. Nesse sentido, garantir que todas as pessoas tenham acesso à internet e aos recursos digitais é crucial para que possam participar plenamente da sociedade da informação.

DA ROCHA (2017, p. 04) discorre que:

> No Brasil, com a chegada da internet ocorreu um momento histórico de grande relevância e progresso para a sociedade brasileira. A partir dos avanços tecnológicos surgiram fatores econômicos, sociais, culturais determinantes para inclusão na Era da globalização, porém, quando há inovações e mudanças em um comportamento social, nem sempre surgem somente consequências positivas, as negativas também afloram junto ou após algum tempo." (DA ROCHA, 2017, p. 04)

Outro marco relevante à era digital é a privacidade e a proteção de dados pessoais. A enorme coleta de informações por empresas e governos traz benefícios, como a personalização de serviços, mas também impõe risos importantes à liberdade e à segurança dos indivíduos. A Lei Geral de Proteção de Dados (LGPD), por exemplo, foi criada para garantir que o uso de informações pessoais respeite limites éticos e legais, oferecendo maior transparência e controle aos cidadãos sobre seus dados.

Considerando a deliberalidade do acesso aos dados pessoais sensíveis que os sistemas de informação possuíam, a LGPD preencheu a lacuna legislativa, estabelecendo limites à utilização desses dados, sentido em que NEGRI & KORKMAZ (2019, p. 73) discutem:

> A partir da compreensão dos riscos associados à circulação e ao tratamento dos dados pessoais sensíveis, nomeadamente pela sua aptidão de gerar situações discriminatórias e de desigualdade, é possível se justificar o estabelecimento de um regime jurídico diferenciado com institutos próprios, voltado a essa categoria específica de dados. [...]Nesse sentido, a LGPD estabeleceu em seu artigo 5ºa distinção entre dado pessoal, entendido como "informação relacionada a pessoa natural identificada ou identificável", do dado pessoal sensível que, através de hipóteses específicas, foi definido como sendo aquele "dado pessoal sobre origem racial ou étnica, convicção

> religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natura" (NEGRI & KORKMAZ, 2019, p. 73)

Outros fatores que impactam o princípio da era digital é a liberdade de expressão e o direito à informação, que também fazem parte desse novo paradigma. A internet possibilita a circulação de ideias e informações em uma escala global, fortalecendo a democracia e o pluralismo. No entanto, essa liberdade encontra desafios como a disseminação de notícias falsas e discursos de ódio, que exigem uma regulamentação equilibrada. O desafio é proteger a liberdade de expressão sem comprometer a integridade das informações e dos direitos individuais.

DA ROCHA (2017, p. 10), explica que a liberdade de expressão é um dos direitos personalíssimos, em que o indivíduo pode manifestar-se nas suas mais variadas facetas, e conclui que:

> [...] Essa liberdade engloba adquirir informações, e divulgá-la sem restrições de fronteiras, por qualquer meio de propagação. A liberdade de comunicação se dá na divulgação da informação pelos instrumentos tecnológicos sem a necessidade de prévia autorização do Poder Público em transmitir para a população." (DA ROCHA, 2017, p. 10)

Além disso, os aspectos principiológicos da era digital enfatiza a transparência e a responsabilidade no uso das tecnologias. Organizações públicas e privadas que desenvolvem e aplicam ferramentas digitais, especialmente aquelas baseadas em inteligência artificial, precisam ser transparentes quanto ao funcionamento de seus algoritmos. Assim, é possível evitar discriminações ou manipulações indevidas e promover uma governança justa do ambiente digital.

Por fim, a cooperação e a sustentabilidade digital são elementos fundamentais para enfrentar desafios globais, como segurança cibernética e impactos ambientais das tecnologias. A colaboração entre governos, empresas e sociedade civil é essencial para desenvolver um ambiente digital mais seguro e ético, além de garantir que a expansão tecnológica aconteça de forma sustentável e inclusiva.

Neste diapasão, os princípios da era digital representam um conjunto de diretrizes que busca equilibrar a inovação tecnológica com valores sociais fundamentais. A inclusão, a privacidade, a liberdade de expressão e a transparência são essenciais para que a era digital seja um espaço de oportunidades e não de exclusão ou abuso. Cabe à sociedade, aos governos e às empresas garantir que o progresso digital seja usado de forma responsável e em benefício de

todos. Investigar os fundamentos e implicações desse princípio no contexto científico é crucial para promover uma sociedade mais justa, inovadora e sustentável.

2 ANÁLISE DA LEGISLAÇÃO BRASILEIRA SOBRE CRIMES CIBERNÉTICOS

Com o avanço da tecnologia e a crescente digitalização das interações sociais, econômicas e políticas, a necessidade de uma legislação eficaz para regular o ambiente virtual tornou-se uma prioridade global.

Conforme explica Filho (2000, p.85):

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes), e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou. (FILHO, 2000, p. 85)

Embora a legislação pátria tenha evoluído no sentido de proteger os usuários da internet, em 2019 durante uma audiência pública da Câmara de Deputados, a procuradora da república Neide Mara Cavalcanti Cardoso de Oliveira, explicou que os principais problemas nesses casos são a ausência de legislação sobre crimes cibernéticos; cooperação internacional pouco eficiente; falta de estrutura pericial das polícias em todos os estados e de capacitação suficiente dos órgãos de persecução penal" (Ministério Público Federal, 2019).

No Brasil, os crimes cibernéticos passaram a receber maior atenção jurídica nas últimas décadas, à medida que o uso da internet cresceu exponencialmente e trouxe consigo novos desafios para a segurança pública. A legislação brasileira, embora tenha dado passos importantes na criação de normas específicas para o combate a esses crimes, ainda enfrenta desafios na aplicação e na atualização constante diante da rápida evolução das práticas criminosas digitais.

A primeira grande iniciativa legislativa no Brasil voltada para o combate aos crimes cibernéticos foi a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que ganhou o nome em razão do caso de invasão de privacidade sofrido pela atriz, cujas fotos pessoais foram obtidas ilegalmente e divulgadas na internet, gerando uma grande comoção pública.

A partir desse episódio, a Lei 12.737 foi sancionada, tipificando crimes como a invasão de dispositivos eletrônicos, a violação de dados pessoais e o acesso não autorizado a informações sigilosas. A lei estabeleceu penas de detenção e multa para quem comete esses atos, trazendo

um marco importante para a proteção dos direitos individuais na esfera digital, os quais serão melhor analisados em tópico específico.

A lei traz a clara percepção de que apesar de sucinta, aponta uma maneira de regular e punir as ações criminosas que corriqueiramente ocorrem no ambiente digital. Embora a legislação anterior já traga tipificações destes crimes enquanto ocorridos fora do ambiente virtual, dentro do digital ainda havia lacunas legislativas a serem preenchidas.

O Brasil conta com outro importante arcabouço legal no que tange aos crimes cibernéticos: o Marco Civil da Internet (Lei nº 12.965/2014). O Marco Civil não apenas estabelece diretrizes para o uso da internet no Brasil, como também regula a responsabilidade de provedores de serviços online em casos de práticas criminosas, como o vazamento de dados ou a disseminação de conteúdo ofensivo. Entre suas disposições, o Marco Civil traz regras sobre a neutralidade da rede, a privacidade e a segurança dos usuários, além de obrigar as empresas a manterem registros de acesso a aplicações da internet por um determinado período para auxiliar em investigações criminais.

Sentido em que CASAGRANDE & ALVES (2022, p. 02), pontuam:

> Abordando agora a Lei 12.965/14, também conhecida como Marco Civil da Internet, é o responsável por regularizar o uso da internet no Brasil. Com isso, seu objetivo é estabelecer direitos, deveres e garantias no meio digital. O Marco Civil da Internet traz alguns princípios basilares, como o princípio da liberdade de expressão, o princípio da privacidade e o princípio da neutralidade da rede. Se tratando de crimes praticados contra os consumidores no ambiente virtual, infelizmente práticas ilícitas comuns ocorridas na internet, por hackers e demais fraudadores no intuito de lesar os consumidores que utilizam do comércio eletrônico para adquirir produtos ou serviços, e com isso gera sérios problemas no mercado de consumo em geral. (CASAGRANDE & ALVES, 2022, p. 02)

Esta legislação é ainda mais sucinta que a Lei Carolina Dieckmann, vez que estabelece "princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. " (Brasil, 2014).

Posteriormente, outra legislação relevante foi a Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018), que entrou em vigor em 2020. A LGPD visa regular o tratamento de dados pessoais por parte de empresas e órgãos públicos, estabelecendo regras claras sobre a coleta, uso e armazenamento de informações. A lei busca proteger a privacidade dos cidadãos, impondo penalidades severas para o uso inadequado de dados e criando a Autoridade Nacional de Proteção de Dados (ANPD) para supervisionar seu cumprimento. Em um contexto de

crimes cibernéticos, a LGPD desempenha um papel crucial, pois qualquer vazamento ou uso não autorizado de dados pode ser caracterizado como infração.

SANTINI (2019, p. 28) interpõe que:

> Ademais, não se pode deixar de mencionar o papel central que o consentimento ocupa entre os fundamentos da LGPD. Tanto que, diferentemente do Código Civil que prevê apenas anulação no caso de vício de consentimento, a Lei Geral de Proteção de Dados sanciona, no Artigo 9º, §1º, a mesma hipótese com nulidade. Em consequência disso, as empresas devem se esforçar para que os seus contratos sejam um instrumento efetivo de esclarecimento e, dessa forma, a anuência dos titulares dos dados seja livre e consciente. Para isso, é importante que constem nos contratos, por exemplo, considerações sobre a forma, a duração e a finalidade específica do tratamento e/ou Compartilhamento de dados, além de informações acerca do Controlador de Dados, dos direitos do titular e das responsabilidades dos agentes que realizarão o tratamento. (SANTINI, 2019, p. 28)

No entanto, apesar de avanços significativos, a legislação brasileira ainda enfrenta desafios. A própria aplicação da Lei Carolina Dieckmann tem sido limitada, especialmente diante da complexidade das infrações cibernéticas e das dificuldades técnicas de identificação e localização dos criminosos. A investigação de crimes cibernéticos requer uma infraestrutura tecnológica robusta e profissionais capacitados, o que muitas vezes não é acessível a todas as delegacias ou instâncias judiciais. Além disso, a internet é um ambiente global, e muitas atividades criminosas são realizadas por indivíduos ou grupos fora das fronteiras nacionais, o que complica ainda mais a aplicação das leis brasileiras.

Bem como CASAGRANDE & ALVES (2022, p. 04) concluem:

> Verificou-se que ainda há uma dissonância entre as diferentes áreas do poder público para definir o foro competente para julgar crimes cibernéticos. Com isso, a hipótese do trabalho de que ainda há uma lacuna a ser preenchia no ordenamento Brasileiro, se tratando do ambiente virtual, se confirmou, visto a divergência da jurisprudência para competência do julgamento de crimes virtuais. (CASAGRANDE & ALVES, 2022, p. 04)

Outro ponto de atenção está relacionado à necessidade de atualização constante das leis. A rapidez com que surgem novas modalidades de crimes cibernéticos, como o *ransomware*, ou mesmo o uso indevido de inteligência artificial para fraudes e manipulações, exige uma legislação dinâmica. O processo legislativo, contudo, é por vezes moroso e não acompanha a velocidade da evolução tecnológica, criando brechas que podem ser exploradas pelos criminosos.

A legislação brasileira sobre crimes cibernéticos tem avançado de maneira significativa nas últimas décadas, com leis como a Lei Carolina Dieckmann, o Marco Civil da Internet e a LGPD representando marcos importantes para a proteção de direitos no ambiente digital. No entanto, ainda há desafios a serem superados, especialmente no que diz respeito à aplicabilidade efetiva dessas normas e à necessidade de constante atualização. Com o cenário digital em

constante evolução, o Brasil precisa continuar investindo na capacitação técnica de suas instituições e na modernização de seu arcabouço jurídico para proteger seus cidadãos contra as ameaças crescentes no mundo virtual.

3 EXEMPLO DE CASO: LEI CAROLINA DIECKMANN

A Lei Carolina Dieckmann (Lei nº 12.737/2012) foi um marco na legislação brasileira voltada para a proteção da privacidade digital e o combate aos crimes cibernéticos. Sua origem está diretamente relacionada a um incidente envolvendo a atriz Carolina Dieckmann, que trouxe à tona a necessidade urgente de regulamentação específica para lidar com a invasão de dispositivos eletrônicos e a divulgação indevida de dados pessoais.

Em maio de 2011, Carolina Dieckmann teve seu computador pessoal invadido por hackers, que roubaram 36 fotos íntimas da atriz. Os invasores exigiram um pagamento para não divulgar as imagens, mas Dieckmann recusou-se a ceder à chantagem. Como resultado, as fotos foram publicadas na internet, causando grande comoção pública e gerando uma ampla discussão sobre a fragilidade das leis brasileiras no que diz respeito à proteção de dados pessoais no ambiente digital.

Onde POMPEU (2022, p. 24) relembra:

> Um marco que impulsionou a constituição de uma lei específica foi o caso da atriz global Carolina Dieckmann, que teve seu computador invadido e seus arquivos pessoais subtraídos, os criminosos começaram a chantageá-la para que fosse feito o pagamento da quantia de dez mil reais (R$ 10.000,00), para que suas fotos de teor 24 íntimo não fossem expostas na web, mas como a atriz não cedeu e denunciou a polícia, teve várias fotos íntimas vazadas e espalhadas através das redes sociais. (POMPEU, 2022, p. 24)

Na época, o Brasil não possuía uma legislação específica que tratasse de crimes cibernéticos, como a invasão de computadores e a violação de dados pessoais. As medidas legais disponíveis para punir os responsáveis eram limitadas, já que o Código Penal brasileiro não estava preparado para lidar com esse tipo de crime, típico de uma sociedade cada vez mais digitalizada.

O caso de Carolina Dieckmann atraiu grande atenção da mídia e da sociedade, impulsionando a discussão sobre a criação de uma legislação que abordasse diretamente os crimes cibernéticos. A pressão popular e a repercussão do caso foram fundamentais para a aceleração do processo legislativo, que já vinha debatendo a necessidade de regulamentar as atividades ilícitas no ambiente virtual.

Com o apoio de vários setores da sociedade, o projeto de lei que viria a se tornar a Lei nº 12.737/2012 foi rapidamente aprovado no Congresso Nacional. Sancionada em dezembro de 2012 pela então presidente Dilma Rousseff, a lei passou a vigorar em abril de 2013.

Crespo (2013, p. 59,):

> A ação judicial promovida por Carolina deparou-se, porém, com um obstáculo jurídico, o mesmo que vem atenuando a punição em casos semelhantes que ocorreram há mais de uma década no Brasil. "Se eu invadisse uma máquina e me valesse de informações confidenciais para ter um proveito financeiro, eu poderia responder por concorrência desleal, por extorsão, mas não pela invasão". [...], por isso, os invasores responderão por crimes que a legislação brasileira já tipifica: furto, extorsão e difamação." (CRESPO, 2013, p. 59)

A crescente dependência da tecnologia e o uso massivo da internet tornaram o ambiente digital um espaço fértil para crimes cibernéticos, expondo usuários a diversas ameaças, como invasões de privacidade e roubo de informações. No Brasil, um marco importante para a proteção da privacidade no ambiente *online* foi a criação da Lei Carolina Dieckmann (Lei nº 12.737/2012). O episódio gerou um debate nacional sobre a vulnerabilidade digital e levou à criação de um dispositivo legal específico para coibir invasões e violações de privacidade por meio de dispositivos eletrônicos.

Além de punir a invasão de dispositivos, a lei também visa proteger a integridade e privacidade das vítimas, tratando com severidade a divulgação indevida de informações pessoais. A legislação representa um avanço ao criar um dispositivo específico para combater práticas que, até então, não encontravam respaldo adequado no Código Penal brasileiro.

A Lei Carolina Dieckmann foi um passo significativo para o Brasil no combate a crimes cibernéticos, atendendo à crescente demanda por segurança digital em um país onde o uso da internet e de dispositivos eletrônicos se expande rapidamente. Além disso, o caso trouxe maior conscientização sobre a importância de proteger dados pessoais no ambiente digital, incentivando o uso de práticas mais seguras, como senhas fortes e o uso de antivírus.

Sob a análise de CARNEIRO, SANTOS & EDLER (2022, p. 2066):

> A criação da Lei Carolina Dieckmann trouxe uma maior segurança aos usuários de equipamentos eletrônicos, pois a lei trouxe em seu texto uma previsão legal a fim de penalizar os infratores que cometem crimes dentro da seara digital. Mas para que tal Lei fosse elaborada houve um acontecimento anterior que possibilitou a realização deste feito. (CARNEIRO, SANTOS & EDLER, 2022, p. 2066)

No entanto, a aplicação da lei encontrou alguns desafios. Um dos principais problemas enfrentados pelas autoridades brasileiras é a dificuldade técnica de identificar e localizar os infratores, uma vez que a maioria dos crimes cibernéticos é cometida de forma anônima e pode

envolver indivíduos ou grupos localizados fora do Brasil. A própria estrutura policial do país, em muitos casos, não dispõe dos recursos tecnológicos e da capacitação necessária para lidar com a investigação de crimes digitais, o que acaba dificultando a aplicação eficaz da lei.

O que ocorrera com a atriz em 2012, não é um fato isolado, embora tenha ganhado grande repercussão dada a sua vida pública, DELLA VALLE (2013), inclusive relembra o ocorrido:

> No mês de maio de 2012 Carolina Dieckmann teve seu e-mail violado através de uma invasão realizados por crackers (criminoso que invade um sistema de segurança a fim de quebra-lo de forma ilegal ou sem ética) do interior de minas gerais, os quais baixaram fotos intimas da mesma. Posteriormente os crackers divulgaram essas imagens na internet e concomitantemente por meio de chantagens solicitaram um valor de R$10.000,00 (dez mil) reais para que aquelas imagens fossem apagadas da internet." (DELLA VALLE, 2013).

Outro ponto crítico é que a legislação, por mais que tenha sido inovadora em seu tempo, já começa a mostrar sinais de desatualização. O cibercrime evolui rapidamente, com o surgimento de novas práticas criminosas, como o uso de *ransomware*, fraudes financeiras mais sofisticadas e até o uso de inteligência artificial para cometer crimes. Embora tenha sido eficaz para tipificar crimes de invasão de privacidade digital, a supramencionada lei, não aborda todos os aspectos de segurança digital que são fundamentais no cenário atual.

A Lei Carolina Dieckmann foi um marco importante no cenário jurídico brasileiro, respondendo a uma demanda crescente por proteção da privacidade no ambiente digital e ajudando a preencher uma lacuna legislativa até então existente. Apesar de ter trazido avanços significativos, como a tipificação de crimes de invasão de dispositivos eletrônicos, sua aplicação ainda enfrenta desafios, principalmente relacionados à identificação de criminosos e à evolução constante das práticas criminosas no mundo virtual.

A Lei Carolina Dieckmann (Lei n.º 12.737/2012), trouxe importantes alterações no Código Penal brasileiro relacionadas a crimes cibernéticos. A motivação para a criação dessa lei foi um caso envolvendo a atriz Carolina Dieckmann, que teve fotos pessoais roubadas de seu computador e divulgadas na internet.

As principais mudanças da Lei Carolina Dieckmann no Código Penal foram a criação dos artigos 154-A e 154-B, que criminalizam a invasão de dispositivos informáticos e o acesso não autorizado a dados alheios. A lei estabelece que:

> *Invasão de dispositivo informático*
> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:

> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 1° Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
> § 4° Na hipótese do § 30, 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.
> § 5° Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> 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
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
> **Ação penal**
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos." (BRASIL, 2012)

A alteração trazida pela Lei nº 12.737/2012 foi fundamental para adaptar a legislação brasileira às novas ameaças tecnológicas, tipificando e prevendo punições específicas para crimes cibernéticos que até então não eram contemplados no Código Penal.

O caso que deu origem à lei não apenas impulsionou a criação de uma norma específica, mas também evidenciou a necessidade de maior conscientização sobre a segurança digital entre os usuários. À medida que os crimes cibernéticos se tornam mais complexos, a legislação brasileira deve continuar a se adaptar para oferecer uma proteção mais abrangente e eficaz no combate às ameaças digitais, fortalecendo tanto o arcabouço jurídico quanto os mecanismos de aplicação da lei.

4 DEFINIÇÃO E TIPOLOGIA DE CRIMES CIBERNÉTICOS

Com o avanço das tecnologias e a crescente digitalização de diversas atividades humanas, a sociedade contemporânea enfrenta novos desafios no campo da segurança e da legalidade. Um dos mais notórios desses desafios são os crimes cibernéticos, também conhecidos como cibercrimes, que envolvem atividades ilegais realizadas por meio de dispositivos eletrônicos conectados à internet ou a redes de computadores. Esses crimes podem ter como alvo indivíduos, empresas ou até mesmo governos, resultando em prejuízos financeiros, sociais e psicológicos.

A natureza jurídica dos crimes cibernéticos refere-se à sua classificação dentro do direito penal e à sua função no ordenamento jurídico. Esses crimes possuem peculiaridades que os diferenciam de delitos tradicionais, mas sua essência é similar, a proteção de bens jurídicos relevantes por meio da aplicação de normas penais, o qual pode ser compreendido como "natureza transnacional" (ROCHA, 2023, p. 06).

De igual modo, OLIVEIRA (2024, p. 02) compreende que:

> [...] a natureza transnacional da internet e das comunicações digitais torna complicada a atribuição de jurisdição e a coordenação entre as autoridades de diferentes países. Isso muitas vezes resulta em lacunas na aplicação da lei e na impunidade dos perpetradores, incentivando ainda mais a prática de crimes virtuais. (OLIVEIRA, 2024, p. 02)

Os crimes cibernéticos integram o direito penal material, pois preveem condutas típicas (descritas em lei) relacionadas ao uso de tecnologias da informação e comunicação.

A definição de crimes cibernéticos pode ser amplamente descrita como qualquer atividade ilegal que envolve o uso de tecnologias digitais para alcançar um fim criminoso. Isso inclui desde a invasão de sistemas e redes, o roubo de dados sensíveis, até fraudes financeiras e a disseminação de conteúdos maliciosos, como vírus e *malwares*.

O autor ROCHA (2023, p. 06) compreende este crime como:

> [...] uma ampla gama de atividades ilícitas, como invasões de sistemas, fraudes eletrônicas, roubo de dados pessoais, phishing, espionagem cibernética, disseminação de malware, entre outros. Essas ações são realizadas por indivíduos ou grupos que exploram as vulnerabilidades do mundo digital para obter benefícios financeiros, prejudicar outras pessoas, empresas e até mesmo governos. (ROCHA, 2023, p. 06)

Neste sentido, o legislador criou a norma incriminadora para crimes cibernéticos, tipificados no art. 154 – A do Código Penal, estabelecendo:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa." (BRASIL, 2021, sem página definida)

A característica principal desses crimes é o ambiente em que ocorrem: o mundo digital, que oferece tanto a oportunidade para sua execução quanto a dificuldade de rastreamento dos infratores. Nesse sentido, os cibercriminosos muitas vezes se beneficiam do anonimato e da dificuldade de localização, o que desafia as autoridades em suas tentativas de controle e punição.

Deste modo, NASCIMENTO (2019) aponta o conceito da INTERPOL, para a definição de crimes cibernéticos, discorrendo:

> "A melhor conceituação para o cibercrime seria a atividade criminosa ligada diretamente a qualquer ação ou prática ilícita na internet. Ainda, pode se dizer que são

> crimes com utilização de computadores e internet, com fins de fraudar sistemas de comunicação, segurança de computadores e redes corporativas. As empresas, atualmente, são as mais visadas, por conter informações sigilosas que podem gerar retorno financeiro em grande escala" (NASCIMENTO, 2019)

Os sujeitos do crime cibernético são os agentes envolvidos na prática ou na condição de vítimas do delito. Em crimes cibernéticos, esses sujeitos podem ser pessoas físicas, jurídicas ou até sistemas automatizados, dada a natureza do ambiente digital.

SANTOS (2020, p. 65) discorre:

> "A jurisdição brasileira sente enorme dificuldade em identificar os sujeitos ativos dos crimes virtuais, uma vez que a quantidade de usuários é cada vez maior. Nota-se, então, que o responsável pela infração é conhecedor de técnicas especializadas e amplo entendedor do mundo informático, o que facilita a ação." (SANTOS, 2020, p. 65)

A legislação penal estabelece de forma indireta dois tipos de sujeitos do crime, o sujeito ativo e passivo. O sujeito ativo é aquele que realiza a conduta criminosa. No caso dos crimes cibernéticos, que pode ser qualquer indivíduo que pratique a ação criminosa, como os hackers (têm conhecimento técnico avançado e exploram vulnerabilidades) e crackers (subvertem sistemas com intenção maliciosa), ou até mesmo usuários comuns que realizam atos ilícitos como a disseminação de fake news ou calúnia.

No que tange ao sujeito ativo, a legislação não é específica, no entanto, o art. 1º do Código Penal: "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal." (BRASIL, 1940) que reflete o princípio da legalidade e pressupõe que o crime é uma ação ou omissão realizada por uma pessoa física, de igual modo, o art. 18 estabelece que o crime pode ser doloso (de forma intencional) ou culposo (por negligência, imprudência ou imperícia), os quais somente se aplicam aos sujeitos que praticam o ato ilícito.

Explica SANTOS (2020, p. 66) que:

> "É bastante comum que quando se trata de delitos virtuais, a sociedade tenha a ideia de que tais práticas sejam realizadas apenas por profissionais ou experts, isto é, os sujeitos ativos mais conhecidos como Hackers ou Crackers. Todavia, a globalização tem cooperado enormemente na popularização dos sistemas de informação, o que tem provocado uma nova onda de crimes virtuais por aqueles que não possuem um domínio tecnológico aprofundado." (SANTOS, 2020, p. 66)

A exemplo disto, empresas e pessoas jurídicas podem ser consideradas sujeitos ativos quando utilizam sistemas ou estratégias digitais para práticas ilícitas, como envio de malware ou exploração indevida de dados pessoais (sob responsabilidade de seus administradores).

No que tange ao sujeito passivo é aquele que sofre a lesão ao bem jurídico protegido. No caso dos crimes cibernéticos, pessoas físicas ou jurídicas que têm os seus direitos de privacidade, honra e patrimônio invadidos, e os seus bens tangíveis ou intangíveis violados.

Para Júlio Fabrinni Mirabete (2008, p. 114), "o sujeito passivo podem ser duas ou mais vítimas, como estabelecido no artigo 147 do Código Penal: "ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave", esse crime é comum nas redes virtuais, podendo ter ao mesmo tempo duas ou mais vítimas. "

Além dos sujeitos diretamente envolvidos, podem haver sujeitos que, de forma indireta, participam ou são impactados como provedores de serviços de internet (que podem ser obrigados a colaborar com investigações); plataformas digitais (como redes sociais que hospedam conteúdo ilícito ou criminoso).

A identificação dos sujeitos em crimes cibernéticos é crucial para sua responsabilização penal e para determinar a melhor forma de reparação dos danos causados. A análise depende de investigações técnicas e, muitas vezes, cooperação entre diversos setores e países, o que retoma a natureza transnacional destes crimes.

Os crimes cibernéticos podem ser classificados em diversas categorias, dependendo de suas técnicas e objetivos. Uma das mais comuns é a divisão entre crimes que têm como alvo as máquinas, ou seja, os próprios sistemas e redes de computadores, e aqueles que têm como meio esses sistemas, visando prejudicar diretamente as pessoas ou instituições. Dentro dessas divisões, a tipologia dos crimes cibernéticos se torna ampla e variada. Assim diz AGLIARDE (2002, p. 02) dispõe que:

> A velocidade estrondosa do avanço da tecnologia, principalmente nos meios de comunicação e telemática, faz com que a sociedade também evolua, o que leva o crescimento de condutas não reguladas ou não previstas. Ao direito cabe a missão compreender e acompanhar essas inovações e acima de tudo garantir a manutenção do Estado Democrático de Direito. Procuramos diferenciar os crimes informáticos nas suas ramificações. O grande desafio é a tipificação de condutas desvaloradas que configurariam os chamados crimes puros da Internet, que se opõe aos crimes comuns, já tipificados na legislação penal vigente. (AGLIARDE, 2002, p. 02)

Entre os crimes contra sistemas e redes de computadores, destaca-se o *hacking*, onde indivíduos ou grupos acessam de forma não autorizada sistemas de computação para modificar, roubar ou destruir dados. Também nessa categoria estão os ataques *DDoS (Distributed Denial of Service)*, que buscam sobrecarregar um sistema, interrompendo sua funcionalidade ao inundá-lo com um tráfego excessivo de dados.

No que tange a definição e tipificação destes crimes BRITO (2020, p. 06) pontua de forma assertiva:

> Os crimes cibernéticos podem ser classificados em: virtuais puros, mistos e comuns. O Crime virtual puro seria a conduta ilícita, cuja atenta o hardware e/ou software de um computador, ou seja, tanto a parte física quanto a parte virtual. Já o Crime virtual misto

> utiliza a Internet para realizar a conduta ilícita, e visa, muitas vezes, as transações ilegais de valores de contas correntes. Por fim, temos o Crime virtual comum, o qual é utilização da Internet apenas como um instrumento para realização de crimes, estes normalmente especificados no Código Penal, como, por exemplo, distribuição de conteúdo pornográfico infantil por diversos meios, espionagem, violação de autorização, falsificação de dados, vazamento indevido de informação, sabotagem do computador e muitos outros meios. (BRITO, 2020, p. 06)

De igual modo, ORRIGO & FILGUEIRA (2015, p. 04) definem a tipologia destes crimes:

> Os crimes cibernéticos próprios são aqueles em que o agente, para cometer um delito, necessita do computador, ou seja, o computador é o meio de execução essencial. Os bens jurídicos afetados, pelos crimes cibernéticos próprios são os dados armazenados em outra máquina ou rede. O delito é cometido por meio do computador e se consuma também pelo meio informático. Na nossa legislação um exemplo é a Invasão de Dispositivo Informático Já os crimes cibernéticos impróprios, também são cometidos por meio do computador, porém o bem jurídico ofendido aqui pode ser afetado de "n" maneiras, não necessariamente com a utilização do computador, ou seja, não é essencial a máquina, o delito atinge o mundo físico, diverso da informática. São exemplos de crimes impróprios tipificados na nossa legislação: Calúnia; injúria; difamação; ameaça; furto; apropriação indébita; estelionato; dano; violação ao direito autoral; pedofilia; crime contra a propriedade intelectual. Observe que todos eles podem ser cometidos sem o uso do computador, mas também é possível comete-los usando o computador como meio. (ORRIGO & FILGUEIRA, 2015, p. 04)

O Código Penal Brasileiro já prevê modalidades de crimes cibernéticos, os quais são tipificados em várias leis, ademais o próprio códex aborda certos tipos de delitos, dentre eles, a modalidade de furto qualificado e estelionato cibernético os quais são previstos respectivamente nos artigos 155, § 4º e art.171 do Código Penal, que trata de roubo de dados para obter vantagens financeiras, como transferências bancárias indevidas. Pode ter agravantes, resultando em penas mais altas, de acordo com a situação.

O acesso não autorizado a sistemas, embora menos específico, o acesso não autorizado pode ser tratado como violação de privacidade, configurando um delito contra a intimidade.

Difamação, Calúnia e Injúria, que já são previstos nos artigos 138, 139 e 140 do Código Penal, são crimes comuns em redes sociais e em outros meios digitais, onde uma pessoa ofende a honra ou divulga informações falsas sobre outra.

Divulgação não autorizada de imagens ou vídeos íntimos, que constitui publicar ou compartilhar imagens íntimas sem consentimento é um crime grave, o qual o Art. 218-C do Código Penal estabelece:

> Art. 28- C - Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça

> apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia. (BRASIL, 1940)

No que tange a fraudes e *phishing*, embora não exista uma lei específica para *phishing*, ele pode ser enquadrado como estelionato. Os criminosos enviam mensagens fraudulentas para obter informações financeiras, o que na percepção de TIESO & SANTOS (2020, p. 03) essa modalidade é amplamente empregada por *hackerse crackerse* consiste em um método comum de obtenção fraudulenta de dados, estabelecem ainda que:

> O ataque é geralmente direcionado a diversas pessoas, organizações ou sistemas de informação. Seu objetivo é induzir os destinatários a acreditarem em mensagens falsas enviadas por e-mail, redes sociais, plataformas etc., muitas vezes acompanhadas de anexos que solicitam atualizações de cadastros, alterações de senhas ou verificação de informações pessoais. (TIESO & SANTOS, 2020, p. 03)

De igual modo, a interrupção de Serviço e Ataques DDoS que podem afetar o funcionamento de sistemas, como em ataques de negação de serviço (DDoS), onde o Art. 266 do Código Penal institui que "interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento", o qual incorre a pena de detenção, de um a três anos, e multa.

Outro tipo importante é o que afeta diretamente as pessoas e instituições em termos financeiros. Fraudes digitais como o *phishing*, onde criminosos se passam por instituições confiáveis para roubar informações sensíveis como senhas e números de cartões de crédito, são extremamente comuns, onde SILVA (2021, p. 15) explica: "A "spear – phishing" atinge especificamente a segurança da empresa que a pessoa trabalha, através de campanhas que chamam a atenção do funcionário, que acaba atingindo a organização." (SILVA, 2021, p. 15)

Em um contexto semelhante, crimes como o *ransomware* destacam-se por bloquear o acesso a sistemas ou arquivos, exigindo pagamento de resgate para que as vítimas recuperem suas informações.

O Tribunal de Justiça do Distrito Federal e Territórios (TJDFT, 2021) estabelece que este tipo de crime se enquadra na modalidade de estelionato digital, que foi acrescido no Código Penal Brasileiro pelos § 2º-A, § 2º-B e § 3º do artigo 171 do códex, e determina: "A fraude eletrônica ocorre quando o criminoso consegue enganar alguém, por meio de redes sociais, contatos telefônicos, correio eletrônico falso ou qualquer outro meio fraudulento, a fornecer dados confidenciais, tais como, senhas de acesso, bancos ou número de cartão de crédito ou débito. " (TJDFT, 2021)

Há ainda os crimes que afetam a privacidade e os dados pessoais, como o roubo de identidade e o vazamento de dados. Nesses casos, os criminosos obtêm e divulgam informações sensíveis de pessoas ou empresas, frequentemente com o objetivo de extorsão ou para cometer outros delitos, como fraudes.

Outros tipos de crimes cibernéticos incluem a disseminação de conteúdos ilegais ou ofensivos, como a exploração infantil e a pornografia envolvendo menores. Essas atividades criminosas ocorrem nas partes mais obscuras da internet, o que torna sua detecção e combate extremamente complexos.

Os crimes relacionados a violência Sexual e pornografia Infantil estão dispostos nos Arts. 240 e 241 do Estatuto da Criança e do Adolescente, e incluem armazenamento, compartilhamento e distribuição de conteúdo pornográfico envolvendo menores, onde instituem:

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
> § 1 o Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena.
> § 1º Incorre nas mesmas penas quem:
> I - agencia, facilita, recruta, coage ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena;
> II - exibe, transmite, auxilia ou facilita a exibição ou transmissão, em tempo real, pela internet, por aplicativos, por meio de dispositivo informático ou qualquer meio ou ambiente digital, de cena de sexo explícito ou pornográfica com a participação de criança ou adolescente
> § 2° Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:
> I – no exercício de cargo ou função pública ou a pretexto de exercê-la;
> II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou
> III – prevalecendo-se de relações de parentesco consanguíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento.
> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1 o Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2 o As condutas tipificadas nos incisos I e II do § 1 o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.

> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 1 o A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.
> § 2 o Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:
> I – agente público no exercício de suas funções;
> II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.
> § 3 o As pessoas referidas no § 2 o deste artigo deverão manter sob sigilo o material ilícito referido.
> Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo.
> Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso:
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Nas mesmas penas incorre quem:
> I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso;
> II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita.
> Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais. " (BRASIL, 2002)

Estas delimitações trazidas pelos artigos 240 e 241 do ECA são essenciais para proteger crianças e adolescentes de situações de abuso e exploração sexual, vez que estabelecem penas para qualquer envolvimento em crimes relacionados à pornografia infantil, seja pela produção, compartilhamento ou até pela posse desse conteúdo. Isso desestimula tanto a criação quanto a circulação de material ilegal e reforça o compromisso de proteger os direitos da infância e adolescência.

Acerca dos cibercrimes envolvendo a exploração infantil e a pornografia, CARLETE & OBREGON (2020, p. 06) explicam:

> Em virtude da globalização, as comunicações ao redor do mundo se estreitaram, especialmente a partir da internet. Ao longo dos anos, essa ferramenta passou por diversos aperfeiçoamentos no mundo inteiro, possibilitando uma velocidade mais rápida no tráfego na rede mundial de computadores e, consequentemente, a expansão da troca de arquivos entre os usuários." (CARLETE & OBREGON, 2020, p. 06)

No mesmo sentido, DAOUN & BLUM (2005, p. 144) explicam: "Apesar de ser controlada por núcleos de irradiação tecnológica, é certa a noção de que a internet está plantada em um local abstrato, ou melhor, terra de ninguém, logo, a conclusão mais imediata que aflora, está fincada na dificuldade em responsabilizar seu dono. " (DAOUN; BLUM, 2005, p. 144).

MARTINS (2021, p. 22) estabelece:

> Existe muita dificuldade na investigação dos crimes na internet, segundo a polícia, não há como investigar crimes que não sejam no Brasil, porque existem vários sites estrangeiros, por exemplo, os Estados Unidos, onde é livre, qualquer tipo de manifestação de opiniões e este problema não pode exigir que retire dos sites, assim, o criminoso fica impune de seus crimes. (MARTINS, 2021, p. 22)

Segundo o autor Oliveira "um usuário da web que em sua *home page* publique fotografias ou filmes pornográficos, envolvendo crianças ou adolescentes, certamente terá de responder pelo delito previsto no referido artigo. Não basta, porém, para a configuração, a simples colocação de links capazes de proporcionar o acesso a outras páginas que contenham esse material; o administrador da página remota não é o usuário em questão; não lhe pode ser atribuída a responsabilidade sobre a conduta de terceiro" (OLIVEIRA, 2011, p. 83).

Por fim, os crimes cibernéticos também envolvem questões de propriedade intelectual, como a pirataria de *software* e o compartilhamento ilegal de arquivos, que prejudicam a indústria de entretenimento e de tecnologia ao permitir a cópia e distribuição não autorizada de conteúdo protegido por direitos autorais.

No que tange a consumação e tentativa destes crimes, avanço tecnológico trouxe novos desafios para o Direito Penal. Condutas ilícitas cometidas por meio de dispositivos conectados à internet, têm características que dificultam a identificação do momento em que se consideram consumados ou apenas tentados. A compreensão desses conceitos no ambiente digital é essencial para assegurar a justiça e a segurança no meio virtual.

Prado (2019), que, para os crimes em comento, quando da consumação e tentativa, *in verbis*:

> "Consuma-se o delito com a mera invasão do dispositivo informático ou instalação de vulnerabilidades, sendo desnecessário que haja efetivamente obtenção, adulteração, destruição de dados ou informações, ou obtenção de vantagem ilícita (delito de mera atividade). A tentativa é admissível, e se verifica quando a invasão ou instalação não ocorrem por circunstâncias alheias à vontade do agente." (PRADO, 2019, p. 1073-1074).

A consumação de um crime ocorre quando o resultado previsto no tipo penal é efetivamente atingido, enquanto a tentativa configura-se quando o agente inicia a execução do delito, mas não alcança o resultado por circunstâncias alheias à sua vontade. No âmbito dos

cibercrimes, essa distinção é complexa devido à natureza do meio digital. Por exemplo, a invasão de um dispositivo informático (Art. 154-A do Código Penal) pode ser considerada consumada no momento em que o agente obtém acesso não autorizado.

Contudo, se o sistema de segurança impede a invasão, pode-se falar em tentativa, essa linha tênue exige análises técnicas detalhadas para determinar o estágio em que o crime se encontra.

LIMA (2024, p. 60) pontua:

> "[...]vislumbra-se neste caso um crime formal, o qual se consuma no momento em que o próprio sujeito ativo invade o aparato informático do sujeito passivo, seja através da violação indevida ou instalando vulnerabilidades, não necessariamente ligado à rede mundial de computadores. A tentativa é admissível por se tratar de um delito plurissubsistente, o qual exige pluralidade de sujeitos ativos, fracionando assim o iter criminis." (LIMA, 2024, p. 60)

Além disso, os crimes formais, comuns no ambiente cibernético, como o envio de malwares ou phishing, não exigem um resultado material para serem considerados consumados. O simples envio de um vírus pode configurar o crime, independentemente de ele causar danos. Já em crimes materiais, como fraudes digitais (Art. 171, §2º-A do CP), a consumação depende do efetivo prejuízo à vítima, o que torna a distinção entre tentativa e consumação mais evidente.

Portanto, a análise da consumação e tentativa de cibercrimes é uma questão central no combate à criminalidade digital. A linha que separa ambos os conceitos, embora complexa no ambiente virtual, deve ser constantemente revisitada e ajustada para que o ordenamento jurídico ofereça respostas eficazes e justas. Só assim será possível proteger adequadamente os bens jurídicos no contexto da sociedade da informação.

A sensação de impunidade para os crimes cibernéticos é comum entre as vítimas, embora a legislação penal trate da punibilidade destes crimes.

A punição desses delitos apresenta desafios específicos, devido à natureza transnacional, anônima e complexa do ambiente virtual. Contudo, é indispensável que o sistema jurídico seja eficiente na repressão dessas práticas para garantir a proteção dos direitos fundamentais no mundo digital.

No Brasil, leis como o Marco Civil da Internet (Lei 12.965/2014) e a Lei 12.737/2012 (Lei Carolina Dieckmann) representam avanços no enfrentamento dos cibercrimes. Mais recentemente, a Lei 14.155/2021 agravou penas para fraudes eletrônicas, demonstrando um esforço legislativo para se adaptar às novas modalidades de crime. No entanto, a efetividade

dessas normas ainda é limitada pela dificuldade de fiscalização e pela lentidão na adaptação às mudanças tecnológicas.

A punição dos crimes cibernéticos no Brasil está prevista em diversas legislações que regulamentam condutas ilícitas no ambiente digital, a exemplo do Artigo 154-A, amplamente exposto neste estudo, trata da Invasão de dispositivo informático e traz a pena de reclusão de 1 a 4 anos e multa para quem invadir dispositivo informático de outrem sem autorização, mediante violação de mecanismo de segurança. A pena é aumentada se a invasão resultar em prejuízo econômico, obtenção de conteúdo sigiloso ou controle remoto do dispositivo.

Já o Artigo 171, § 2º-A do Código Penal, alterado pela LGPD, apresenta a fraude eletrônica com pena de reclusão de 4 a 8 anos e multa para quem obtiver vantagem ilícita em prejuízo de outrem, induzindo ou mantendo alguém em erro por meio eletrônico, rede social ou outro meio análogo (BRASIL, 2021).

Previamente, o Código Penal apresenta o art. 266 que versa sobre a interrupção ou perturbação de serviços telegráficos, telefônicos ou de informática com pena de reclusão de 1 a 3 anos e multa; bem como os artigos 198 e 199 que tratam respectivamente da falsificação de documentos particulares com pena de reclusão de 1 a 5 anos e multa e o crime de falsidade ideológica com pena de reclusão de 1 a 5 anos e multa, que também são aplicáveis à informações digitais (BRASIL, 1940).

A Lei 12.965/2014, discorre em seu artigo 12 sobre sanções para quem viola a privacidade ou a segurança de dados na internet, podendo incluir suspensão ou proibição de atividades e multas, *in verbis*:

> "Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
>
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
>
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.
>
> Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País." (BRASIL, 2014)

Outrossim, a LGPD estabelece sanções administrativas, incluindo multas de até 2% do faturamento da empresa, limitada a R$ 50 milhões por infração, para casos de uso ou vazamento indevido de dados pessoais.

> "Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II; [...]." (BRASIL, 2018)

Esses dispositivos formam o arcabouço jurídico brasileiro para a punição de crimes cibernéticos, mas desafios permanecem, como a rápida evolução tecnológica e a necessidade de cooperação internacional em crimes transnacionais.

Outro ponto crucial é a cooperação internacional. Muitos crimes cibernéticos são cometidos de forma transnacional, exigindo articulação entre diferentes países para identificar e punir os responsáveis. Tratados como a Convenção de Budapeste sobre Crimes Cibernéticos têm promovido essa integração, mas desafios persistem, como diferenças nos sistemas jurídicos e na definição dos crimes.

Além disso, é fundamental investir em educação digital e no fortalecimento das forças de segurança cibernética. Ferramentas como inteligência artificial e análise de big data podem ajudar na identificação de criminosos e na coleta de provas digitais. Sem esses investimentos, a punição continuará limitada, prejudicando a eficácia da legislação.

Portanto, a punição dos crimes cibernéticos é essencial para a preservação da ordem jurídica na era digital, mas enfrenta barreiras relacionadas à evolução tecnológica e à necessidade de cooperação internacional. Cabe ao poder público, às instituições e à sociedade civil trabalharem juntos para fortalecer a legislação, melhorar a capacidade investigativa e promover uma cultura de responsabilidade no uso das tecnologias.

CONSIDERAÇÕES FINAIS

O avanço tecnológico e a crescente digitalização de atividades cotidianas trouxeram uma nova e complexa dimensão para o campo da segurança e da legislação. No Brasil, o combate aos crimes cibernéticos vem evoluindo gradualmente, com a criação de leis que buscam proteger a privacidade dos cidadãos e garantir a integridade de suas informações no ambiente digital. A Lei Carolina Dieckmann, o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD)

são exemplos de como o país vem buscando adaptar seu arcabouço legal às novas ameaças virtuais.

No entanto, o panorama legislativo ainda enfrenta desafios significativos. A rápida evolução das técnicas utilizadas por cibercriminosos exige uma legislação ágil, atualizada e eficaz, que possa responder às novas modalidades de ataques digitais, como fraudes financeiras sofisticadas e o uso de inteligência artificial para crimes. Além disso, é necessário fortalecer a infraestrutura técnica e humana para a aplicação dessas leis, garantindo que investigações possam identificar e punir os responsáveis.

A legislação brasileira tem avançado no combate aos crimes cibernéticos, mas precisa continuar a evoluir, incorporando novas tecnologias e promovendo a cooperação internacional, fundamental em um ambiente virtual globalizado. O caminho para uma maior segurança digital exige não apenas aprimoramento legislativo, mas também a conscientização dos cidadãos e o desenvolvimento de políticas públicas que fortaleçam a cultura da proteção de dados no país.

Os crimes cibernéticos são os grandes vilões do ambiente digital, vez que o avanço tecnológico que se atualizada a cada dia buscam de todas as formas blindar ou pelo inibir que estes crimes ocorram, mas a cada adaptação e evolução que o meio digital oferece no sentido e proteger os dados sensíveis de seus usuários, novas estratégias de burlá-la são criadas.

A melhor estratégia para que estes crimes ocorram cada vez menos ou que definitivamente não ocorram são medidas simples que incluem a educação e conscientização para usuários e empresas sobre segurança digital, boas práticas e como identificar tentativas de fraude, a colaboração Internacional, já que os crimes cibernéticos muitas vezes transcendem fronteiras, onde a cooperação entre países, por meio de acordos e compartilhamento de informações, é crucial para enfrentar esses desafios, além de investir em soluções de segurança cibernética, como firewalls, criptografia e inteligência artificial, para proteger sistemas e dados. Vislumbra-se que a legislação e regulamentação brasileira já abordam crimes cibernéticos e buscam sempre garantir que estas sejam eficazes e adaptáveis às novas tecnologias.

REFERÊNCIAS BIBLIOGRÁFICAS

_____, 2021. Lei nº 14.155, de 27 de maio de 2021. Brasília, 27 de maio de2021; 200º da Independência e 133º da República. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 07 Nov. 2024.

Abrão, G. P. (2024). A EFETIVIDADE DA LEGISLAÇÃO BRASILEIRA NA PREVENÇÃO E PUNIÇÃO DE CRIMES CIBERNÉTICOS: REFLEXÕES INSPIRADAS NO UNIVERSO CYBERPUNK. Disponível em: < https://repositorio.pucgoias.edu.br/jspui/handle/123456789/7467 > Acesso em: 16 Nov. 2024.

ACS. **Estelionato.** Tribunal de Justiça do Distrito Federal e Territórios – TJDFT. 2021. Disponível em: < https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/estelionato-1#:~:text=A%20fraude%20eletr%C3%B4nica%20ocorre%20quando,cart%C3%A3o%20de%20cr%C3%A9dito%20ou%20d%C3%A9bito. > Acesso em 10 Out. 2024.

AGLIARDI, Mauricio O.; KOLLER, Ana CSG; CASTRO, Anderson RA. A evolução dos crimes virtuais na era digital. **Salão de iniciação Científica (14.: 2002: Porto Alegre, RS). Livro de resumos. Porto Alegre: UFRGS, 2002.**, 2002.

BARBAGALO, Fernando Brandini. Cibercriminalidade e crimes informáticos: uma aproximação entre a legislação italiana e brasileira. 2022. Disponível em: < chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.migalhas.com.br/arquivos/2022/10/30FAAEC01AD111_Cyberciminalidade.pdf > Acesso em 15 Set. 2024.

BARBOSA, Mateus Israel Alves Crivinel. Crimes virtuais: a evolução dos crimes cibernéticos e os desafios no combate. 2020. Disponível em: < https://repositorio.pucgoias.edu.br/jspui/handle/123456789/105 > Acesso em: 20 Out. 2024.

Batista, R. F., & Gouveia, J. S. (2023). CRIMES CIBERNÉTICOS FINANCEIROS: A EVOLUÇÃO DO PHISHING ATRAVÉS DA VULNERABILIDADE DO PÚBLICO DIGITAL. *Revista Juris Sertão/Juris Sertão Journal*, *1*(1), 87-111. Disponível em: < https://jurissertao.com.br/index.php/home/article/view/17 > Acesso em: 10 Nov. 2024.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm > Acesso em: 01 Nov. 2024.

BRASIL. Estatuto da Criança e do Adolescente: Lei federal nº 8069, de 13 de julho de 1990. Rio de Janeiro: Imprensa Oficial, 2002. BRASIL. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l8069.htm > Acesso em: 01 Nov. 2024.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm#art2>. Acesso em: 08 Set. 2024.

BRASIL. Lei no 12.965, de 23 Abril de 2014.Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 2014. Disponível em: <http://www.cgi.br/pagina/marco-civil-da-internet-no-brasil/177>. Acesso em: 09 Set. 2024.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidente da República. Disponível em: < https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm > Acesso em: 08 Set. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020].

BRITO, Marcelo Matos. Crimes cibernéticos e a recepção da lei no 12.737/2012 no Brasil. 2020. Disponível em: <https://ri.ucsal.br/items/1ded7eeb-dd99-42ae-ba28-6314a1136158> Acesso em: 10 Out. 2024.

CARLETE, Juliana Barbosa; OBREGÓN, B. M. F. Q. A função do Ministério Público Federal no combate aos crimes de pornografia infantojuvenil na rede mundial de computadores e a importância da adesão do Brasil à Convenção de Budapeste (The role of the Federal Prosecutor's Office in combating crimes of child pornography on the World Wide Web and the importance of. 2020. Disponível em: < https://www.derechoycambiosocial.com/revista061/La_funcion_del_Ministerio_Publico_Federal.pdf > Acesso em: 10 Out. 2024.

CARNEIRO, Lucas Vitor Vitório; SANTOS, Jackson Novaes; EDLER, Gabriel Octacilio Bohn. DIREITO CIBERNÉTICO: O IMPACTO GERADO PELA LEI CAROLINA DIECKMANN NO COMBATE AOS CRIMES VIRTUAIS REALIZADOS CONTRA AS CRIANÇAS E ADOLESCENTES. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 8, n. 11, p. 2061-2080, 2022. Disponível em: < https://periodicorease.pro.br/rease/article/view/7793 > Acesso em: 16 Out. 2024.

CASAGRANDE, Nicollas de Almeida; ALVES, Rodrigo da Silva; DUTRA, Deo Pimenta. Análise da legislação brasileira sobre os crimes cibernéticos:" reflexão sobre a competência para julgamento dos delitos praticados via internet". 2022. Disponível em: < https://dspace.doctum.edu.br/handle/123456789/4468 > Acesso em: 10 Out. 2024.

Cazaroti, T. M. B., & Pinheiro, E. F. (2016). Crimes Cibernéticos. *TCC-Direito*. Disponível em: < http://www.repositoriodigital.univag.com.br/index.php/rep/article/view/203 > Acesso em: 15 Nov. 2024.

Conselho da Europa. **Convenção sobre o Cibercrime (Convenção de Budapeste)**. Budapeste, 23 de novembro de 2001. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Acesso em: 16 nov. 2024.

CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. São Paulo. Ed Saraiva. 2011.

DA ROCHA, Maria Célia Albino. A Era Digital: Restrição À liberdade de expressão. 2017. Disponível em: < http://metodistacentenario.com.br/jornada-de-direito/edicoes-anteriores/9a-jornada-de-pesquisa-e-8a-jornada-em-extensao-do-curso-de-direito/artigos/o-direito-a-privacidade-na-sociedade-da-informacao/e5-01.pdf > Acesso em: 05 Out. 2024.

DAOUN, Alexandre Jean. Crimes informáticos. In: BLUM, Renato M. S. Opice (Coord.). Direito eletrônico – a internet e os tribunais. São Paulo: EDIPRO, 2001.

DE ÁVILA NEGRI, Sergio Marcos Carvalho; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na lei geral de proteção de dados: ampliação conceitual e proteção da pessoa humana. **Revista de Direito, Governança e Novas Tecnologias**, v. 5, n. 1, p. 63-85, 2019. Disponível em: < https://indexlaw.org/index.php/revistadgnt/article/view/5479 > Acesso em: 14 Out. 2024.

DE CAMPOS, Igor Santos; DE MELO, Marcos Túlio. **Os crimes cibernéticos no ordenamento jurídico brasileiro e a pornografia da vingança.** Centro Universitário de Várzea Grande – UNIVAG. Repositório Digital UNIVAG. Várzea Grande – MT. 2018. Disponível em: < https://repositoriodigital.univag.com.br > Acesso em 14 Out. 2024.

DE JESUS ALMEIDA, Jessica et al. Crimes cibernéticos. **Caderno de Graduação-Ciências Humanas e Sociais-UNIT-SERGIPE**, v. 2, n. 3, p. 215-236, 2015. Disponível em: < https://periodicos.grupotiradentes.com/cadernohumanas/article/view/2013/1217 > Acesso em: 10 Out. 2024.

de Melo, M. T., da Luz, J. C. F., & Nóbrega, P. M. A TUTELA JURÍDICA SOBRE OS CRIMES CIBERNÉTICOS. Disponível em: < https://egov.ufsc.br/portal/sites/default/files/a_tutela_juridica_sobre_os_crimes_ciberneticos.pdf > Acesso em: 15 Nov. 2024.

DE OLIVEIRA, Bruna Machado et al. Crimes virtuais e a legislação brasileira. 2017. Disponível em: < https://core.ac.uk/download/pdf/229767447.pdf > Acesso em 02 Out. 2024.

DE SIENA, David Pimentel Barbosa. Lei Carolina Dieckmann e a definição de "crimes virtuais". 2013. Disponível em: < https://jus.com.br/artigos/24406/lei-carolina-dieckmann-e-a-definicao-de-crimes-virtuais > Acesso em 10 Out. 2024.

DELLA VALLE, James. Lei Carolina Dieckmann entra em vigor nesta terça-feira Leia mais em: https://veja.abril.com.br/tecnologia/lei-carolina-dieckmann-entra-em-vigor-nesta-terca-feira/. 2013. Veja. Disponível em: < https://veja.abril.com.br/tecnologia/lei-carolina-dieckmann-entra-em-vigor-nesta-terca-feira/>. Acesso em: 14 Out. 2024.

GARCIA, Alline Tavares. O DIREITO À INTIMIDADE E A FRÁGIL PRIVACIDADE DA ERA DIGITAL: uma análise sobre os crimes cibernéticos e a eficácia da lei Carolina Dieckmann. 2017. Disponível em: < https://monografias.ufma.br/jspui/handle/123456789/1651 > Acesso em: 10 Out. 2024.

GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. Boletim IBCCRIM, v. 8, 2000.

Janeiro: Lume Juris, 2011.

Lima, D. M. F. D. N. (2024). Os desafios da investigação nos crimes cibernéticos. Disponível em: < https://repositorio.ufpb.br/jspui/handle/123456789/31393 > Acesso em: 16 Nov. 2024.

Marques, K. K. C., Jacob, R. S. R. C., & Marques, H. R. CRIMES INFORMÁTICOS CONTRA INSTITUIÇÕES DIGITAIS: DA NECESSIDADE DE EQUIPARAÇÃO ENTRE PENAS PARA O CRIME DE ROUBO COMETIDOS EM AMBIENTES FISICO E VIRTUAL. Disponível em: < https://pergamum.ucdb.br/pergamumweb/vinculos/ooooa/oooooaee.pdf > Acesso em 22 Out. 2024.

MARTINS, M. N. (2021). CRIMES CIBERNÉTICOS: O COMBATE À PORNOGRAFIA INFANTIL NO AMBIENTE VIRTUAL. Disponível em: < http://65.108.49.104/handle/123456789/386 > Acesso em 01 Nov. 2024.

MAUES, Gustavo Brandão Koury; DUARTE, Kaique Campos; DA SILVA CARDOSO, Wladirson Ronny. Crimes virtuais: uma análise sobre a adequação da legislação penal brasileira. 2018. Disponível em: < http://www.publicacoes.unirios.edu.br/index.php/revistarios/article/view/326 > Acesso em: 08 Out. 2024.

MINISTÉRIO PÚBLICO FEDERAL. MPF defende adesão do Brasil à Convenção de Budapeste em audiência pública na Câmara. Brasília: Secretaria de Comunicação Social, 2019. Disponível em: < https://www.mpf.mp.br/pgr/noticias-pgr/mpf-defende-adesao-do-brasil-a-convencao-de-budapeste-em-audiencia-publica-na-camara > Acesso em: 10 Out. 2024.

MIRABETE, Julio Fabbrini. Manual de direito penal, vol. 2: parte especial. 25. Ed. São Paulo: Atlas, 2008.

MIRABETE, Julio Fabbrini. Manual do Direito Penal: parte geral. 24 ed. São Paulo: Atlas, 2008.

MOLITOR, Heloísa Augusta Vieira; VELAZQUEZ, Victor Hugo Tejerina. BREVE PANORAMA SOBRE A LEGISLAÇÃO APLICADA NOS CRIMES ELETRÔNICOS. **Revista de Direito, Governança e Novas Tecnologias**, v. 3, n. 2, p. 81-96, 2017. Disponível em: < chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://core.ac.uk/download/pdf/210565892.pdf > Acesso em: 15 Set. 2024.

NASCIMENTO, Samir. Cibercrimes: Conceito, modalidades e aspectos jurídicos-penais. Âmbito Jurídico. 2019. Disponível em: < https://ambitojuridico.com.br/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/ > Acesso em 10 Out. 2024.

Oliveira, C. H. B. D. (2024). Discussões jurídicas acerca do estelionato virtual: evolução, características e combate. Disponível em: < http://repositorio.upf.br/handle/riupf/2723 > Acesso em: 15 Nov. 2024.

OLIVEIRA, Eugênio Pacelli de. Curso de Processo Penal. 15ª Ed. Ver e atual. Rio de

ORRIGO, G. M. A., & FILGUEIRA, M. H. B. (2015). Crimes cibernéticos: uma abordagem jurídica sobre os crimes realizados no âmbito virtual. *Encontro de Iniciação Científica (ETIC)*, *11*(11). Disponível em: < https://egov.ufsc.br/portal/sites/default/files/crimes_ciberneticos_uma_abordagem_juridica_sobre_os_crimes_realizados_no_ambito_virtual.pdf >. Acesso: 22 Out. 2024.

PINHEIRO, Patrícia Peck. Direito digital global e seus princípios fundamentais. Revista Jurídica, São Paulo, p. 46-47, 2016.

POMPEU, Ana Luiza Brandão Calil et al. Crimes Cibernéticos: A Ineficácia da Lei Carolina Dieckmann. 2022. Disponível em: < http://65.108.49.104/handle/123456789/509 > Acesso em: 12 Out. 2024.

PRADO, L.R. **Curso de Direito Penal Brasileiro. – 17. ed.** – Rio de Janeiro: Forense, 2019.

Rocha, G. A. (2023). Crimes cibernéticos características, peculiaridades da investigação e as ameaças na ''rede mundial de computadores''. Pontífica Universidade Católica de Goiás.

Disponível em: < https://repositorio.pucgoias.edu.br/jspui/handle/123456789/8043 > Acesso em: 15 Nov. 2024.

SANTINI, Barbara et al. A eficácia da Lei Geral de Proteção de Dados (LGPD). **Dados Internacionais de Catalogação na Publicação (CIP)-(Câmara Brasileira do Livro, SP, Brasil)**, v. 19, 2019. Disponível em: < https://apphotspot.com.br/wp-content/uploads/elementor/forms/OAB-PE-Oque-est%C3%A3o-fazendo-com-meus-dados-LGPD.pdf#page=19 > Acesso em: 29 Set. 2024.

Santos, K. H. F. (2020). Cibercrime: uma breve análise dos sujeitos e principais delitos virtuais. *CRIMES DIGITAIS*, 58. Disponível em: < https://repositorio.uniceub.br/jspui/bitstream/prefix/14602/1/Crimes%20digitais.pdf > Acesso em: 16 Nov. 2024.

SILVA, Eva Cristina de Souza. Proteção contra os crimes cibernéticos no Brasil: a necessidade de uma legislação específica e atualizada. 2021. Disponível em: < https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/1487/1/Eva%20Cristina%20de%20Souza%20Silva%20-%20Artigo%20-.pdf > Acesso em: 10 Out. 2024.

SILVA, Lucas. FRAUDE ELETRÔNICA: FURTO OU ESTELIONATO?(DIREITO). **Repositório Institucional**, v. 1, n. 1, 2023. Disponível em: < https://revistas.icesp.br/index.php/Real/article/view/3973 > Acesso em: 21 Out. 2024.

SILVA, Milene Meneze. **Crimes Cibernéticos:** Uma Análise da Lei Carolina Dieckmann. Universidade São Judas Tadeu – Campus Mooca. São Paulo – SP. 2023.

SILVA, Norma Lucia; UEHARA, Milton. A evolução da tecnologia digital: seus impactos no setor bancário. **Enciclopédia Biosfera**, v. 16, n. 29, 2019. Disponível em: < https://www.conhecer.org.br/ojs/index.php/biosfera/article/view/343 > Acesso em: 08 Out. 2024.

Teles, L. M. A. (2024). Reflexões Sobre os Desafios Enfrentados Pelo Direito Criminal Diante dos Crimes Perpetrados na Internet. Disponível em: < https://repositorio.ufu.br/handle/123456789/42101 > Acesso em: 16 Nov. 2024.