UNIVERSIDADE FEDERAL DA PARAÍBA
DIRETÓRIO DE CIÊNCIAS JURÍDICAS
CURSO DE GRADUAÇÃO EM DIREITO

Suellen Juliany Neves Santana

Criminalidade cibernética: desafios na regulação do ciberespaço

SANTA RITA
2025

SUELLEN JULIANY NEVES SANTANA

Criminalidade cibernética: desafios na regulação do ciberespaço

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Diretório de Ciências Jurídicas da Universidade Federal da Paraíba, como exigência parcial da obtenção do título de Bacharel em Ciências Jurídicas.

Orientador: Prof. Dr. Felipe Negreiros Deodato.

SANTA RITA

2025

Catalogação na publicação
Seção de Catalogação e Classificação

S232c Santana, Suellen Juliany Neves.
Criminalidade cibernética: desafios na regulação do ciberespaço / Suellen Juliany Neves Santana. - Santa Rita, 2025.
51 f.

Orientação: Felipe Augusto Forte de Negreiros Deodato.
TCC (Graduação) - UFPB/CCJ/DCJ-SANTA RITA.

1. Crimes cibernéticos. 2. Ciberespaço. 3. Internet. 4. Direito penal. 5. Legislação penal. I. Deodato, Felipe Augusto Forte de Negreiros. II. Título.

UFPB/DCJ/CCJ-SANTARITA CDU 34

Elaborado por ANA BEATRIZ DE OLIVEIRA ABRANTES SILVA - CRB-15/596

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS JURÍDICAS
DIREÇÃO DO CENTRO
COORDENAÇÃO DE MONOGRAFIAS
DEPARTAMENTO DE CIÊNCIAS JURÍDICAS
DISCIPLINA: TRABALHO DE CONCLUSÃO DE CURSO

CCJ Centro de Ciências Jurídicas

ATA DE DEFESA PÚBLICA DE TRABALHO DE CONCLUSÃO DE CURSO

Ao vigésimo segundo dia do mês de Setembro do ano de dois mil e vinte e cinco, realizou-se a sessão de Defesa Pública do Trabalho de Conclusão do Curso de Direito intitulado "Criminalidade cibernética: desafios na regulação do ciberespaço", do(a) discente(a) **SUELLEN JULIANY NEVES SANTANA**, sob orientação do(a) professor(a) Dr. Felipe Augusto Forte de Negreiros Deodato. Após apresentação oral pelo(a) discente e a arguição dos membros avaliadores, a Banca Examinadora se reuniu reservadamente e decidiu emitir parecer favorável à APROVAÇÃO, de acordo com o art. 33, da Resolução CCGD/02/2013, com base na média final de 10,0 (dez). Após aprovada por todos os presentes, esta ata segue assinada pelos membros da Banca Examinadora.

Dr. Felipe Augusto Forte de Negreiros Deodato

Dr. José Ernesto Pimentel Filho

Dra. Werna Karenina Marques de Sousa

RESUMO

O presente trabalho aborda a crescente popularização dos meios virtuais e suas implicações no âmbito jurídico, destacando a transformação das relações sociais e a necessidade de adaptação das leis para acompanhar a evolução da sociedade. Os produtos digitais oferecem facilidades em diversas áreas, como pesquisa e relacionamentos, mas também trazem novas ameaças e vulnerabilidades. Os crimes cibernéticos, que podem ocorrer em qualquer local do mundo, são um desafio tanto para a investigação quanto para a aplicação da lei, devido à dificuldade de identificar o infrator e a competência legal envolvida. Estes crimes, que utilizam tecnologias avançadas, podem gerar grandes impactos financeiros e sociais e afetam de forma crescente a população brasileira. Com um estudo crítico partindo de fontes bibliográficas e documentais, o projeto busca analisar como a legislação penal brasileira protege seus cidadãos contra crimes cibernéticos e quais alternativas podem ser adotadas para melhorar essa defesa, considerando as complexidades envolvidas na investigação e repressão desses delitos.

Palavras-chave: Crimes cibernéticos; ciberespaço; internet; legislação penal; Direito Penal.

ABSTRACT

This paper addresses the growing popularity of virtual media and its implications for the legal sphere, highlighting the transformation of social relations and the need to adapt laws to keep pace with societal developments. Digital products offer benefits in various areas, such as research and relationships, but they also pose new threats and vulnerabilities. Cybercrimes, which can occur anywhere in the world, pose a challenge for both investigation and law enforcement due to the difficulty in identifying the offender and the legal jurisdiction involved. These crimes, which utilize advanced technologies, can generate significant financial and social impacts and increasingly affect the Brazilian population. Through a critical study based on bibliographic and documentary sources, the project seeks to analyze how Brazilian criminal law protects its citizens against cybercrimes and what alternatives can be adopted to improve this defense, considering the complexities involved in investigating and prosecuting these crimes.

Keywords: Cybercrimes; cyberspace; internet; criminal legislation; Criminal Law.

Sumário

1 Introdução

Com a popularização dos meios informativos, mecanismos tecnológicos e espaços virtuais, foram remodeladas as relações sociais e, consequentemente, as necessidades regulatórias do meio jurídico, tendo em vista que é inevitavelmente moldado de acordo com a progressão da sociedade e necessidades emergentes. É sabido que os produtos virtuais proporcionam diversas facilidades ao usuário, tanto no âmbito da pesquisa, quanto no de relacionamentos, em que as conexões podem ser facilitadas e são promovidas de forma instantânea.

A internet tem demonstrado sua capacidade de reorganizar as estruturas de poder e de influenciar o comportamento humano, especialmente no que diz respeito à forma como os indivíduos se expõem socialmente. No entanto, o uso de dispositivos como intermediadores gera uma falsa sensação de comodidade para o usuário e de invencibilidade para o infrator, seja por seu caráter global ou pela ausência de moderadores mais explícitos.

Dessa forma, com essa tendência e fluidez do meio, também são desenvolvidas novas ameaças e vulnerabilidades, propiciando o aperfeiçoamento de crimes mais complexos em uma velocidade mais eficiente. Paralelamente, estes crimes cibernéticos não estão restritos ao território de um único país, suscitando uma maior dificuldade na localização de determinados dados e identificação de competência, bem como na aplicação do Direito de cada localidade.

Não são raras as ocasiões em que os usuários da internet se deparam com crimes de injúria, calúnia, crimes de falsa identidade, divulgação de materiais confidenciais, apologia ao estupro virtual e ataques através de mecanismos desenvolvidos por hackers com vírus que infectam desde dispositivos pessoais até empresariais e, devido às informações obtidas, empreendem uma extorsão.

Esses crimes também podem ser chamados de crimes virtuais e geralmente são delitos que utilizam aparatos de alta tecnologia para sua perpetração, no entanto, podem se manifestar através atos aparentemente simples e cotidianos, desde que facilitem a troca de dados.

À vista disso, é possível afirmar que os crimes cibernéticos apresentam complexidades tanto na parte investigativa quanto repressiva, isto porque a vítima pode estar localizada em determinada jurisdição de uma autoridade policial e o infrator em outro Estado, consequentemente em competência diferente daquele. Do

mesmo modo, é possível que o infrator modifique os dados referentes à sua localização e torne seu rastreio uma tarefa extremamente difícil.

Por conseguinte, a presente pesquisa tenciona analisar e compreender o tratamento jurídico direcionado para a regulação de dados e os crimes cibernéticos, não só quanto à legislação penal brasileira, mas também buscando direcionamentos frente aos diplomas normativos internacionais, como a Convenção de Budapeste. Paralelamente, serão observadas as dificuldades quanto à definição de competência e aplicação do Direito Penal de cada localidade.

Além disso, visa tratar acerca do crime de pornografia infantil, cujo combate enfrenta significativos desafios, tanto na identificação correta de crianças e adolescentes em imagens, quanto na modificação constante dos arquivos para formatos que necessitam de mecanismos investigativos mais complexos para superar os meios convencionais de detecção. Tendo em vista que esse é um dos crimes cibernéticos mais graves e bastante frequentes no país, exigindo uma resposta firme do ordenamento jurídico brasileiro, é imprescindível analisar os dispositivos legais aplicáveis e formas de combate.

Dessa forma, é possível analisar como é realizada a defesa dos interesses dos usuários da rede mundial de computadores perante crimes cibernéticos e qual a alternativa para suprir a demanda de proteção do ofendido brasileiro. É cristalina a necessidade de uma maior conscientização acerca dos principais crimes virtuais e pesquisa acerca das legislações vigentes a serem aplicadas nos casos típicos, bem como suas dificuldades de concretização e possíveis soluções aplicáveis frente à criminalidade no ambiente cibernético.

A partir de pesquisas exploratórias e descritivas, visando discorrer e analisar fontes bibliográficas e documentais, com coleta de dados tanto em textos legais quanto em artigos científicos através de busca entre os conteúdos gratuitos no portal de Periódicos CAPES utilizando os termos “cibercrimes”, “crimes virtuais”, “cibersegurança”, “crimes cibernéticos” e “dificuldade no combate de cibercrimes” e interpretação crítica das informações coletadas, considerando a complexidade do limite entre a segurança jurídica dos usuários no meio virtual e proteção de sua intimidade.

A escolha dos artigos se deu após a leitura do resumo, introdução e conclusão dos trabalhos, buscando trabalho com embasamento sólido e bem desenvolvidos. Alguns dos trabalhos apresentavam os critérios necessários, mas

foram excluídos para evitar redundância em relação ao tema, considerando a escolha de pesquisas similares. A base de periódicos da CAPES foi escolhida para colher a bibliografia do presente trabalho pela pluralidade de fontes de qualidade, diversidade de materiais e ferramentas de busca avançada, além de seu uso facilitado.

O presente trabalho pretende desempenhar uma investigação acerca da criminalidade cibernética para descrição e análise dos principais desafios na regulação do ciberespaço e enfrentamento à criminalidade cibernética para promover esclarecimento e compreensão no que diz respeito à segurança relativa às novas tecnologias. Assim como, de forma pormenorizada, a identificação dos tipos de crimes cibernéticos, estudo das legislações vigentes sobre o assunto e a avaliação das dificuldades de aplicação de políticas regulatórias.

2.1 Crimes cibernéticos e seus mecanismos

Antes de tratar sobre os cibercrimes em sua pluralidade, é preciso compreender o conceito de crime, que de acordo com Rogério Greco pode ser conceituado como um fato típico, ilícito e culpável. Esse fato típico pode ser dividido em conduta dolosa ou culposa e comissiva ou omissiva, resultado da ação, nexo de causalidade entre a conduta e o resultado e tipicidade, que pode ser formal e conglobante (GRECO, 2015).

O elemento da ilicitude diz respeito ao antagonismo entre a conduta do agente e o ordenamento jurídico e a culpabilidade seria o juízo que é feito sobre a conduta, que contém entre suas considerações a imputabilidade, o potencial consciente acerca da ilicitude do fato e exigibilidade de conduta diversa (GRECO, 2015).

Paralelamente, Zaffaroni (2015) conceitua o delito como uma conduta humana individualizada através de um tipo, que determina sua proibição por não estar de acordo com causa que justifique cobertura por princípios jurídicos, sendo contrária ao ordenamento, consequentemente antijurídica. Assim, pela possibilidade e exigibilidade de o sujeito ativo agir de outra maneira em determinada circunstância, há reprovabilidade (ZAFFARONI, 2015).

Essa visão estratificada, que divide o conceito de crime em três elementos, teoria tripartite, é a mais aceita pelo ordenamento brasileiro atualmente (SANTOS,

2017). Com isso, cabe analisar o conceito de crimes cibernéticos, seus mecanismos e elementos principais.

Os crimes cibernéticos, cibercrimes ou crimes virtuais são delitos cometidos por meio de equipamentos de alta tecnologia (SILVA, 2006). Com isso, o autor da transgressão já não precisa mais estar presente para perpetrar o crime, bastando que seja praticado pela rede mundial de computadores. É necessário pontuar que nesses casos não deixa de ser necessária a tipicidade da conduta para que o infrator seja indiciado (SANTOS, 2017).

Entre as denominações utilizadas para tratar sobre os crimes realizados através da rede mundial de computadores e demais sinônimos de crimes virtuais, o termo mais apropriado conforme a Convenção de Budapeste seria de fato “crimes cibernéticos” (SANTOS, 2017). Isto é, os crimes cibernéticos podem ser definidos como condutas típicas, que possuem os pressupostos da ilicitude, culpabilidade e são sucedidas no ambiente virtual, ou ciberespaço (SANTOS, 2017).

> Os bens jurídicos lesionados por meio da internet podem ser tanto o sistema informático em si mesmo, os dados pessoais arquivados ou disponibilizados por meio do sistema informático, como ainda outros bens jurídicos lesionados em razão do conteúdo veiculado por meio do sistema informático (publicidade enganosa e abusiva, pornografia infantil), e que devem ser tipificados penalmente. (Santos, 2018)

O ambiente cibernético é um novo espaço social, vinculado ao real de forma permanente e paralela, trazendo consequências reais para além do âmbito particular da internet (SIQUEIRA *et al.*, 2021), sendo ele uma extensão do espaço geográfico. Considerando as novas Tecnologias de Informação e Comunicação (TICs) desenvolvidas:

> O ciberespaço se caracteriza pela convergência digital consubstanciada na integração de diversos formatos e dispositivos em um mesmo “lugar”, ou seja, trata-se de um espaço conceitual inserido no ambiente das TICs. Assim, dada a continuidade dos avanços tecnológicos, atualmente o ciberespaço não pode ser visto tão somente como um espaço de interconexão de computadores, mas sim em todas as suas variações como tablets, smartphones, laptops, vídeos games, smartvs, etc, tornando uma característica desse espaço a multidisciplinaridade. (Siqueira et al., 2021)

A questão com o ciberespaço é sua imaterialidade, esse mundo virtual tornou mais difícil a aplicação da correta lei penal, expandindo esse território para um

ambiente global com transcendência dos limites territoriais (CONTE; SANTOS, 2008).

> Ademais, há que se ter em mente que os delitos perpetrados em ambiente virtual possuem caráter transnacional, uma vez que atingem diversos países, simultaneamente, que somado ao caráter global do ciberespaço, faz surgir a necessidade de uma nova análise acerca do exercício da aplicação da lei penal no espaço. (Conte; Santos, 2008)

Para além do espaço em que os cibercrimes são cometidos, é pertinente conceituar algumas de suas modalidades conhecidas. Os crimes cibernéticos podem ser *strictu sensu*, quando necessitam da internet para que sejam cometidos, contando não apenas com a tecnologia, como um vírus utilizado para sequestrar dados eletrônicos e conteúdos armazenados pela vítima (SILVA, 2006).

Já o segundo tipo, *lato sensu*, geralmente são realizados através da tecnologia, mas não precisam de internet para o seu sucesso (SILVA, 2006). Exemplo disso são os aparelhos modificados que se passam por maquinetas para clonar cartões e armazenar as senhas dos usuários. Entre as classificações encontradas acerca dos crimes cibernéticos, a mais utilizada os divide entre crimes cibernéticos comuns ou impróprios e crimes cibernéticos autênticos ou próprios (SANTOS, 2017).

Os crimes cibernéticos impróprios ou comuns são conceituados por Marco Aurélio Rodrigues Costa (1997) como:

> São todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta a perpetração de crime comum, tipificável na lei penal, ou seja, a via eleita do sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta.

É possível citar como exemplo o caso do crime de calúnia, tipificado no artigo 138 do Código Penal (BRASIL, 1940), que consistem em acusar alguém erroneamente de ter cometido um crime, atribuindo esse fato criminoso à vítima publicamente. Esse delito pode ser perpetrado através da tecnologia no ambiente virtual, mas não necessita desse mecanismo para que seja realizado.

Por outro lado, os crimes de informática próprios, autênticos ou puros, ocorrem quanto tanto o meio quanto o alvo da infração é o computador:

> São aqueles em que o sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas. Entendemos serem os elementos que compõem a informática o "software", o "hardware" (computador e periféricos), os dados e sistemas contidos no computador, os meios de armazenamento externo, tais como fitas, disquetes, etc. Portanto são aquelas condutas que visam exclusivamente a violar o sistema de informática do agente passivo. (Costa, 1997)

Nesse cenário, o autor tem o objetivo de sabotar o sistema da vítima e obter o controle do dispositivo, podendo tanto acessar informações quanto provocar uma falha no sistema. Em alguns casos, para além das classificações supracitadas, é possível falar em crimes de informática mistos, aos quais geralmente são aplicadas tanto normas da lei penal comum quanto disposições da lei penal de informática, conforme Marco Aurélio Rodrigues Costa (1997): “São todas aquelas ações em que o agente visa a um bem juridicamente protegido diverso da informática, porém, o sistema de informática é ferramenta imprescindível a sua consumação.”.

> a. O crime virtual puro corresponderia à conduta ilícita voltada para o sistema do computador, para a violação do equipamento e de seus componentes, inclusive dados e sistemas (software, hardware e meios de armazenamentos);
> b. Os crimes virtuais mistos aqueles em que o uso de meios computacionais é condição necessária para a efetivação da conduta, embora o bem jurídico visado seja diverso do informático (transferência ilícita de valores ou “*salemislacing*” – retiradas diárias de pequenas quantias de milhares de contas bancárias); (Santos, 2018)

Não obstante, atualmente os crimes cibernéticos mistos são muitas vezes incorporados ao conceito de crimes impróprios, considerando que o sistema informacional é utilizado apesar de o alvo não estar incluso em seus dados (SANTOS, 2017).

2.1.1 Dos sujeitos

Entre as principais dificuldades da jurisdição brasileira está a de identificar e localizar os sujeitos ativos dos crimes virtuais, tanto pelo potencial tecnológico especializado dos autores, quanto pela quantidade de usuários dos sistemas virtuais. O sujeito ativo é o indivíduo que comete a ação ilícita através dos equipamentos informáticos e podem ser conceituados de formas diferentes de acordo com sua atuação (SANTOS, 2020).

No polo passivo, é encontrado o cidadão que é alvo do crime, ou seja, a vítima do delito, que pode ser pessoa física ou jurídica, assim como instituição pública ou privada (SANTOS, 2020). Entre os sujeitos presentes no polo ativo, os mais populares são os *hackers*, as principais figuras no tocante à habilidade da navegação virtual entre dispositivos e sistemas, conhecidos pelo grande conhecimento e experiência na computação, não necessariamente de forma criminosa (SANTOS, 2017).

> Na mesma linha da analogia seguem os hackers. Indivíduos com alto conhecimento técnico-informático podem usar suas habilidades para achar falhas no sistema, seja a fim de modificá-los ou melhorá-los, seja até mesmo notificar a empresa ou grupo a qual o sistema pertence para que este não fique vulnerável a um ataque virtual. (Santos, 2017)

Há ainda o paralelo estabelecido de que a melhor tradução para o termo *hacker* seria “fuçador” visto que pode adentrar e invadir sistemas, obter dados e informações e ainda assim não danificar ou deixar vestígios (CRESPO, 2011). Nesse cenário, é imprescindível conceituar os *crackers*, que são *hackers* que utilizam suas habilidades para decifrar e “quebrar” códigos, seja em benefício próprio ou para o prejuízo de pessoas e entidades.

> O cracker é aquele que, basicamente, “quebra” um sistema de segurança, invadindo-o. Fanáticos pelo vandalismo, também adoram “pichar” páginas da web deixando, na maioria das vezes, mensagens de conteúdo ofensivo e racista. Vale frisar que geralmente os criminosos da informática são mesmo os crackers, embora não sejam os únicos. A expressão consagrada, porém, para criminosos que utilizam computadores como arma é hacker. (Crespo, 2011)

As formas de invasão e comprometimento de sistemas computacionais são, em grande medida, determinadas pela criatividade e pela capacidade de inovação dos agentes maliciosos. Não se trata de um conjunto fixo e estático de técnicas, mas sim de um campo em constante transformação, no qual novas estratégias surgem cotidianamente com o propósito de ampliar o alcance das infecções digitais (SANTOS, 2017).

Tais estratégias exploram, sobretudo, características humanas, como a curiosidade natural, a confiança em mensagens aparentemente legítimas e a tendência ao descuido diante de situações rotineiras. Dessa forma, os atacantes conseguem inserir softwares maliciosos em dispositivos de um número expressivo

de vítimas, aproveitando-se de fragilidades que transcendem apenas o aspecto técnico e alcançam também a dimensão comportamental.

Entre os métodos mais difundidos estão as chamadas “iscas digitais”, que consistem em comunicações fraudulentas destinadas a persuadir o usuário a executar determinada ação, como abrir anexos, clicar em links ou fornecer dados pessoais (SANTOS, 2017). Um exemplo clássico e de grande reconhecimento público é o envio de mensagens eletrônicas que informam falsamente que o destinatário teria sido contemplado com valores vultosos ou prêmios inexistentes (SANTOS, 2017).

Apesar de sua simplicidade, esse tipo de fraude permanece eficaz, revelando a força dos mecanismos de engenharia social como instrumento para a propagação de ataques cibernéticos. De acordo com a pesquisa DataSenado, 24% dos brasileiros acima de 16 anos foi vítima de golpes perpetrados em ambientes virtuais em 2024 (SENADO, 2024).

O Professor Marcelo Crespo (2011) trata ainda de tipos específicos de estelionatários, que são os infratores que realizam compras virtuais através de cartões de crédito de terceiros, atacando os sistemas das administradoras de cartões, furtando números e posteriormente vazando e disponibilizando os dados para aumentar o funil de suspeitos no ambiente cibernético, que são chamados de *carders*.

Dentre os sujeitos ativos, estão os *phreakers*, especialistas em telefonia que utilizam seu conhecimento para realizar desde ligações gratuitas, utilizando o plano e registro de outra pessoa daquela operadora, até escutas telefônicas utilizando o computador para monitoramento e um método de clonagem que o permite ouvir as conversar a partir de seu próprio telefone (CRESPO, 2011). Já os *wannabes*, são os indivíduos que possuem certo conhecimento sobre sistemas e equipamentos, mas não chegam a conseguir *hackear* um sistema (CRESPO, 2011).

2.1.2 Das principais ameaças no ciberespaço

Entre as principais ameaças derivadas da difusão das novas tecnologias e interações no ambiente da rede mundial de computadores, surgiram práticas que impactam diretamente a segurança dos usuários, como os *softwares* maliciosos. Os *malwares*, que são a forma contraída de *malicious software*, são programas

empregados para o roubo, modificação e deterioração do sistema informacional da vítima (SANTOS, 2017).

São utilizados instrumentos para atrair o usuário e conseguir sua permissão para que o programa malicioso consiga infectar a máquina, como a camuflagem em mensagens e comunicações enganosas que parecem inofensivas e corriqueiras (SANTOS, 2017). Além disso, é possível que a vítima caia nesse golpe de outras formas, de acordo com Humberto de Oliveira Pedra dos Santos (2017), “os crackers também escondem esses softwares nocivos em programas aparentemente inofensivos, nos quais o usuário é levado a instalar o *malware* juntamente com o software que deseja obter”, sendo inúmeras as formas para se infiltrar no sistema alvo.

Os *malwares* mais comuns são os vírus de computador, que possuem a capacidade de se replicar, precisando apenas de algo que realize sua ativação (CRESPO, 2011). Entre os programas maliciosos que se assemelham com os vírus, mas são mais perigosos estão os *worms*, que podem ser chamados de vermes (SANTOS, 2017). Nesses *malwares*, não é necessária nenhuma ação ou iniciativa do usuário para sua perpetuação, são *softwares* completos que se autorreplicam e não precisam de hospedeiro para se expandir (WENDT; JORGE, 2013).

> O jeito mais comum de um *worm* infectar uma computador é através de anexos hostis em e-mails. O *worm* se autorreplica e envia mais e-mails para todos na lista de contatos do usuário atacado, expandindo-se indefinidamente e assim por diante. Geralmente os *worms* exploram as vulnerabilidades de computadores que estão com seus programas desatualizados. *Worms* são de difícil identificação, sendo notados apenas quando o computador está lento devido a enorme quantidade de cópias que o *worm* gerou de si mesmo. (Santos, 2017)

Ainda nesse âmbito, é importante tratar sobre os *botnets*, que ocorre quando há uma rede de computadores infectados por *malwares* e com isso geram abertura para que os cibercriminosos controlem os dispositivos de forma remota sem que os usuários legítimos dos computadores sequem tenham conhecimento de que as instruções recebidas pelo sistema vêm de outro local (WENDT; JORGE, 2013).

Humberto de Oliveira Pedra dos Santos (2017) esclarece que esse tipo de investida contra sistemas de informação é denominado DDoS, sigla em inglês para *Distributed Denial of Service*, que em português significa “Ataque Distribuído de Negação de Serviço”. Trata-se de uma técnica utilizada por agentes maliciosos com

o objetivo de sobrecarregar os servidores de uma aplicação ou de um site por meio do envio simultâneo e massivo de requisições provenientes de diversos dispositivos comprometidos (WENDT; JORGE, 2013).

Ao gerar um tráfego artificialmente elevado e muito acima da capacidade de resposta da infraestrutura alvo, o ataque provoca instabilidade, lentidão ou mesmo a completa indisponibilidade do serviço. Com essa ferramenta, o DDoS é um dos recursos mais empregados para inviabilizar o acesso a páginas de grande porte, principalmente as que desempenham funções críticas ou que apresentam alta visibilidade na internet (CASSANTI, 2014).

Existe, ainda, entre os programas maliciosos, o chamado “Cavalo de Troia” ou *trojan*, que se camufla como um simples programa enquanto é formado com códigos que objetivam o prejuízo do usuário paralelamente à execução de processos corriqueiros, Moisés de Oliveira Cassanti (2014) ainda trata do processo de infiltração do dispositivo, que consiste nas etapas:

> Instalação de Keyloggers (histórico de teclas): esta ferramenta é muito usada por atacantes cuja finalidade é capturar tudo que a vítima digita, também capturando os cliques do mouse, printscreen da tela e vídeo da webcam (podendo ver tudo que o usuário está fazendo). Assim, é possível descobrir suas senhas do Facebook, Skype, Twitter, chats e, lógico, capturar números de contas, senhas e outras informações antes delas serem criptografadas por dispositivos de segurança do sistema financeiro. Depois de tudo capturado, é enviado (geralmente por e-mail) para alguém em algum lugar, que analisa o que foi digitado e levanta as informações necessárias(...) Instalação de Trojan-Downloader: faz download de outros vírus para seu computador. Instalação de Trojan-Banker: seu objetivo PRINCIPAL é obter dados de autenticação de usuário e validação de transações em sistema de internet banking. Inclusão de Backdoors (porta dos fundos): é um utilitário de administração remota que, uma vez instalado, permite acesso de usuário e controlá-lo através de uma rede ou da internet (...)

Além das modalidades citadas, é possível citar, ainda, os *ransomwares*, mais especializados e que visam criptografar o sistema do usuário e impedir seu acesso, deixando apenas um pedido de resgate para conseguir certo montante (CASSANTI, 2014).

2.1.3 Da pornografia infantil

Entre os exemplos de crimes cibernéticos em que o computador é o dispositivo utilizado como instrumento para o crime, não de armazenamento, como

também de divulgação e compartilhamento, está a pornografia infantil. Esse crime é disciplinado pelo Estatuto da Criança e do Adolescente (ECA) com pena de reclusão de 4 a 8 anos e multa para a hipótese de produção e reprodução dos registros explícitos envolvendo crianças ou adolescentes (BRASIL, 1990).

Para o caso de transmissão, disponibilização, publicação ou distribuição, por qualquer meio, seja virtual ou não, a pena é de reclusão de 3 a 6 anos consoante o estabelecido no artigo 241 – A do ECA (BRASIL, 1990). O armazenamento dos conteúdos também é tipificado na legislação e punível com reclusão de 1 a 4 anos e multa (BRASIL, 1990).

Nesse cenário, é relevante pontuar que “pedofilia” é um termo representativo para uma doença, conforme disposição da *World Health Organization* (WHO, 1993), que tem como sintoma desordem mental ou desvio sexual reconhecido pela atração por crianças ou adolescentes, não sendo a doença, por si só, um crime (CAIADO; CAIADO, 2018). Dessa forma, é possível afirmar que não existe crime de pedofilia e que “o crime de pornografia infantojuvenil nem sempre é praticado por pedófilos” (SILVA, 2017).

Apesar das ferramentas utilizadas nos dias atuais para identificação de arquivos que contenham esse tipo de conteúdo pornográfico,

> Ainda faltam soluções mais avançadas de buscas em redes P2P, especialmente ao buscar arquivos que não sejam somente aqueles já categorizados. Essa atualização é bastante relevante, tendo em vista que os predadores podem alterar os arquivos de forma que não possuam uma correspondência com bibliotecas de *hash*. (Caiado; Caiado, 2018)

Diante das novas adversidades, hoje em dia os indivíduos suspeitos de envolvimento com pornografia infantojuvenil podem ser identificados por múltiplos métodos, que vão além da detecção automatizada e incluem, por exemplo, investigadores disfarçados que estabelecem contato com os criminosos, tanto no ambiente virtual quanto no presencial (CAIADO; CAIADO, 2018). Após a identificação de um suspeito, é possível solicitar um mandado para que seus computadores e demais dispositivos eletrônicos sejam examinados e analisados (CAIADO; CAIADO, 2018).

Entre as dificuldades encontradas no combate da propagação de pornografia infantil, está a detecção de adolescentes:

> A experiência prática mostra que a identificação da existência de imagens de crianças em arquivos de pornografia infantojuvenil (PI) é fácil, enquanto a de adolescentes é mais complexa, tendo em vista um possível desenvolvimento mais rápido do que usual. Isso ocorre com mais frequência em adolescentes do sexo feminino, que podem ser confundidas com pessoas adultas, situação esta amplificada nos casos de arquivos com menor resolução gráfica. (Caiado; Caiado, 2018)

Para uma abordagem efetiva no que diz respeito ao combate desse abuso, é possível combinar métodos tecnológicos disponíveis de análise de imagens, não só categorizando os arquivos, mas também buscando outros potenciais bancos de informações que possuem o mesmo tipo de material:

> A técnica de MMFF usa uma combinação de métodos disponíveis como detecção de pele, o conceito de visual words e de SentiBank, que respectivamente detectam imagens de pele, olham por vocabulário relacionado à PI e categorizam alguns sentimentos relacionados a crianças sendo exploradas que aparecem na imagem. Sentimentos como medo e raiva são mais comumente encontrados nessas imagens, sendo que, em contraste, esses sentimentos são raramente identificados em outros tipos de pornografia. Dessa forma, podemos achar não apenas arquivos de PI já conhecidos, mas também outros novos. (Caiado; Caiado, 2018)

Com isso, embora os métodos convencionais possam revelar uma quantidade considerável de arquivos de pornografia infantojuvenil, não deixa de ser necessário o desenvolvimento e aplicação de mecanismos automatizados de busca capazes de acompanhar a forma de produção contínua desse material, bem como sua disseminação incessante (CAIADO; CAIADO, 2018). À vista disso, é imprescindível que governos, instituições acadêmicas e setores industriais compreendam de maneira aprofundada as transformações dessas práticas criminosas e estabeleçam uma colaboração contínua e sistemática (CAIADO; CAIADO, 2018).

> O Direito também se transforma e passa à regulação de relações jurídicas novas ou antigas, relações agora em novo formato, e, por consequência, também o Direito Penal precisa ser adaptado às novas realidades, para proteger não somente bens jurídicos individuais, mas também supraindividuais (interesse público, interesse coletivo), dentre os quais a infância. (Santos, 2018)

Tal cooperação visa o desenvolvimento de tecnologias e métodos investigativos inovadores, capazes de potencializar a eficácia das ferramentas disponíveis na detecção de material de pornografia infantojuvenil, assegurando,

simultaneamente, a observância rigorosa dos protocolos forenses e a preservação integral da cadeia de custódia (CAIADO; CAIADO, 2018).

Apenas com essa abordagem integrada será possível enxergar um cenário mais seguro para as crianças, em que todas as ocorrências de abuso sexual e seus efeitos possam ser identificados, documentados e combatidos de forma eficiente, tendo em vista que, de acordo com a Safernet Brasil (2025): “Em 2024, a rede de 55 hotlines, presente em 51 países, detectou a existência de 1.155 páginas diferentes hospedadas no Brasil, o que equivale a 0,05% de todas as páginas contendo material de abuso sexual infantil detectadas no mundo.”.

2.2 Legislações acerca dos crimes cibernéticos

Diante da crescente relevância da internet e da complexidade das relações nela estabelecidas, torna-se cada vez mais necessário assegurar direitos e deveres aos indivíduos que nela participam. Assim, é fundamental aplicar continuamente os princípios oriundos da matriz axiológica constitucional, visando à criação de normas que protejam não apenas o corpo físico, mas também o “corpo eletrônico”, constituído pelos dados e informações pessoais de cada pessoa (TEFFÉ; MORAES, 2017).

As interações no ambiente virtual, assim como em quaisquer outras esferas, devem respeitar rigorosamente os princípios constitucionais, com destaque para o princípio basilar do Estado Democrático de Direito brasileiro: a dignidade da pessoa humana (TEFFÉ; MORAES, 2017). Nesse contexto, o intérprete do direito, à luz da legalidade constitucional, deve priorizar a proteção dos interesses existenciais diante de conflitos ou litígios.

2.2.1 Convenção de Budapeste

Entre os principais dispositivos que tratam dos crimes cibernéticos, está a Convenção sobre o Cibercrime, ou Convenção de Budapeste, que começou a ser assinada em 2001, entrou em vigor em meados de 2004 e passou a vigorar para a República Federativa do Brasil após ratificação no início de 2023 (BRASIL, 2023). A Convenção trata acerca da segurança na internet, fraudes perpetradas nos meios digitais, transgressão aos direitos autorais e disseminação de pornografia infantil nos

meios de comunicação, visando o combate dessas infrações e disciplinando os limites investigativos:

> Convencidos de que a presente Convenção é necessária para impedir ações conduzidas contra a confidencialidade, a integridade e a disponibilidade de sistemas informáticos, redes e dados de computador, bem como para impedir o abuso de tais sistemas, redes e dados, ao prever a criminalização de tais condutas, tal como se encontram descritas nesta Convenção, e ao prever a criação de competências suficientes para combater efetivamente tais crimes, facilitando a descoberta, a investigação e o julgamento dessas infrações penais em instâncias domésticas e internacionais, e ao estabelecer mecanismos para uma cooperação internacional rápida e confiável. (Brasil, 2023)

Para fins informativos, são conceituados na Convenção o “sistema de computador”, que seria qualquer aparelho ou conjunto de aparelhos que estejam relacionados entre si, seja de forma isolada ou em conjunto pela execução de um programa e o “dado de computador”, que é a apresentação de fatos e informações de modo adequado para processamento em um sistema que contenha o programa capaz de fazer o sistema realizar uma tarefa (BRASIL, 2023). Além disso, é importante pontuar a definição apresentada sobre o “provedor de serviços”, que representa qualquer entidade pública ou privada que permita que os usuários se comuniquem mediante um sistema de computador e qualquer outra associação que realize o processamento ou armazenamento de dados de um computador em nome dos serviços ou seus usuários (BRASIL, 2023).

Além da responsabilização, estabelece a cooperação dos provedores de serviço com as autoridades competentes, desde que esteja de acordo com sua capacidade técnica de interceptação e necessidade das providências a serem tomadas. Com essa contribuição, é possível assegurar a confidencialidade, a disponibilidade e a integridade de sistemas informáticos, redes e dados de computador (BRASIL, 2023)

Para mais, sobre o conceito de “dados de tráfego” definido no Decreto nº 11.491 de 2023, trata-se de quaisquer dados de computador referentes a uma comunicação através de um sistema informatizado, gerados por um dispositivo eu seja parte na cadeia de comunicação e que indiquem sua origem, caminho, destino e detalhes acerca da duração ou tipo de serviço oferecido.

Entre os pontos de destaque da Convenção no que diz respeito à aplicação penal, é importante citar que não prevê modalidade tentada de delito, mas sim

apenas crimes dolosos (SANTOS, 2017). Paralelamente, prescreve que os provedores de serviços devem colaborar com a justiça para combater a cibercriminalidade, adotando providências no limite de suas capacidades técnicas, coletando dados de tráfego e os gravando para cooperar com as autoridades competentes (BRASIL, 2023).

Outrossim, é possível que o provedor de serviços sejam compelidos a coletar e gravar informações por meios técnicos em tempo real com a finalidade de ajudar as autoridades competentes em atribuições investigativas (BRASIL, 2023).

A Convenção está estruturada em quatro capítulos principais, sendo o primeiro destinado à definição e ao uso dos termos, o segundo às medidas a serem adotadas em âmbito internacional, o terceiro à cooperação entre os países e o quarto às disposições finais, podendo cada capítulo ser subdividido em seções e estas, por sua vez, em títulos.

No que diz respeito à jurisdição, questão complexa relativa aos crimes cibernéticos, dispõe em seu artigo 22 (BRASIL, 2023):

> 1. Cada Parte adotará medidas legislativas e outras providências necessárias para estabelecer jurisdição sobre qualquer dos crimes tipificados de acordo com os Artigos de 2 a 11 desta Convenção, quando a infração for cometida:
> a. no seu território; ou
> b. a bordo de uma embarcação de bandeira dessa Parte; ou
> c. a bordo de uma aeronave registrada conforme as leis dessa Parte; ou
> d. por um seu nacional, se o crime for punível segundo as leis penais do local do fato ou se o crime for cometido fora da jurisdição de qualquer Parte.

A Convenção de Budapeste também preceitua que a segurança informática é composta por disponibilidade, confidencialidade e integridade das informações dos usuários e sistemas informáticos, visando combater o abuso desses sistemas e redes ao estabelecer criminalização de tais condutas, e a criação de competências que consigam impedir efetivamente esses crimes (BRASIL, 2023). A partir disso, torna-se cada vez mais viável a descoberta, investigação e identificação desses delitos.

Entre os crimes que podem ser disciplinados por cada parte do tratado em seus artigos, está o acesso ilegal, que é o acesso doloso e sem autorização a um sistema de computador de forma total ou parcial, podendo ter como objetivo obter dados de um computador ou contra um sistema que esteja conectado a outro dispositivo (BRASIL, 2023). Sobre a interceptação ilícita e intencional de

transmissões não públicas de dados de computador, dispõe que a medida legislativa pode ser realizada visando eliminar o ato que, por meios técnicos, seja no interior de um sistema informatizado, a partir dele ou em direção a ele e inclui as emissões eletromagnéticas que contenham tais dados (BRASIL, 2023).

A violação de dados, de acordo com o Decreto nº 11.491 (2023), pode incluir a danificação, eliminação, deterioração, alteração ou supressão não autorizada e realizada de forma dolosa nos dados do dispositivo. As partes do tratado são obrigadas, ainda, a adotar medidas legislativas que proíbam e tipifiquem como crime, para além das condutas supracitadas, a produção, venda, aquisição, distribuição ou importação de aparelhos ou equipamentos desenvolvidos para o cometimento de crimes (BRASIL, 2023).

No que tange aos crimes informáticos, delimita que as partes devem adotar medidas e providências que tipifiquem como crimes a falsificação informática e a fraude informática (BRASIL, 2023). A primeira seria delimitada como:

> a inserção, alteração, apagamento ou supressão, dolosos e não autorizados, de dados de computador, de que resultem dados inautênticos, com o fim de que sejam tidos como legais, ou tenham esse efeito, como se autênticos fossem, independentemente de os dados serem ou não diretamente legíveis e inteligíveis. Qualquer Parte pode exigir, para a tipificação do crime, o seu cometimento com intenção de defraudar ou com outro objetivo fraudulento. (Brasil, 2023)

Já a fraude informática tem seu tipo delineado em torno da conduta do indivíduo que der causa de forma dolosa e não autorizada ao prejuízo patrimonial da vítima, que pode ser mediante “qualquer inserção, alteração, apagamento ou supressão de dados de computador”, assim como “qualquer interferência no funcionamento de um computador ou de um sistema de computadores, realizada com a intenção fraudulenta de obter, para si ou para outrem, vantagem econômica ilícita” (BRASIL, 2023).

Quanto aos crimes relacionados ao conteúdo da informação contidos no título 3, há a instrução acerca da pornografia infantil, firmando que as partes comprometidas com a Convenção sobre o Crime Cibernético (2023) devem adotar providências legislativas para as condutas citadas:

> a. produzir pornografia infantil para distribuição por meio de um sistema de computador;

> b. oferecer ou disponibilizar pornografia infantil por meio de um sistema de computador;
> c. distribuir ou transmitir pornografia infantil por meio de um sistema de computador;
> d. adquirir, para si ou para outrem, pornografia infantil por meio de um sistema de computador;
> e. possuir pornografia infantil num sistema de computador ou num dispositivo de armazenamento de dados de computador. (Brasil, 2023)

Visando complementar esse conceito, pornografia infantil engloba material pornográfico que represente visualmente um indivíduo menor de idade envolvido em conduta sexual de forma explícita, uma pessoa que aparente menoridade envolvida em conduta sexual de modo explícito e imagens realísticas retratando um menor envolvido em ato sexual (BRASIL, 2023). Nesse caso, a menoridade é abrangente para todas as pessoas com menos de 18 anos de idade, apesar de as partes possuírem o poder de definir um limite diferente, não é possível que seja inferior a 16 anos (BRASIL, 2023).

Esses delitos já foram tipificados no Estatuto da Criança e do Adolescente no ordenamento brasileiro a partir do artigo 240, que trata da produção, reprodução, registro fotográfico ou em vídeo através de qualquer meio de cena explícita de teor sexual ou pornográfico com a participação de criança ou adolescente (BRASIL, 1990). Estabelece pena também para a venda de conteúdos que contenham tais cenas, assim como o oferecimento e disponibilização destes conteúdos (BRASIL, 1990).

O diploma normativo de nº 8.069 de 1990 também trata da responsabilização penal dos infratores que adotarem as seguintes condutas de acordo com o artigo 241-A, § 1º:

> 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.

2.2.2 Marco Civil da Internet

É imprescindível analisar, no âmbito do presente trabalho, o Marco Civil da Internet, Lei nº 12.965/2014, que disciplina o uso da internet no país, seus princípios e garantias do usuário. Ele começou a ser elaborado ainda em 2009, com uma

consulta pública realizada na internet e tramitando no Congresso Nacional desde 2011 a 2014 (SANTOS, 2017).

Na Lei nº 12.965 de 2014, há a disposição acerca da relação entre o exercício da cidadania e o acesso à internet, constando não só garantias quanto à inviolabilidade da intimidade e vida privada, sua necessária proteção e possível indenização em caso de dano, quanto à inviolabilidade e sigilo do fluxo de suas comunicações pela internet, ou armazenadas e proibição do fornecimento de registros de acesso e conexão a aplicações de internet, salvo previsto em lei ou mediante consentimento (BRASIL, 2014).

Em seu artigo 7º, apresenta os direitos dos usuários de internet no Brasil:

> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização; V - manutenção da qualidade contratada da conexão à internet; VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais; XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet; XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet. (Brasil, 2014)

Entre eles, um dos pressupostos mais recorrentes é o da inviolabilidade da vida privada, que pode gerar obrigação de indenizar proporcional ao dano sofrido pelo usuário (BRASIL, 2014).

> A liberdade d expressão, considerada como liberdade de externar ideias, juízos de valor e as mais variadas manifestações do pensamento, além de já ser amplamente protegida pelo constituinte, apresenta no MCI tutela destacada, sendo considerada um fundamento e um princípio para a disciplina do uso da internet no Brasil e condição para o pleno exercício do direito de acesso. Ao longo do Marco Civil, percebe-se a preocupação do legislador com a comptibilização desses princípios, tendo por fim assegurar que, também na internet, a pessoa humana possa livremente desenvolver sua personalidade. (Teffé; Moraes, 2017)

Outro ponto de destaque é a disponibilização dos dados armazenados pelos provedores apenas em casos necessários para o andamento de investigação após requerimento por ordem judicial, sendo possível seu compartilhamento para terceiros para além desse caso apenas na hipótese de consentimento expresso pelo cliente (BRASIL, 2014).

No que tange aos registros de conexão armazenados pelos administradores de sistemas autônomos, há a determinação de que sejam armazenados em ambiente seguro e controlado por um ano (BRASIL, 2014). Paralelamente, o artigo 15 do Marco Civil estabelece que o provedor de aplicações de internet, constituído como pessoa jurídica, que desempenhe atividade de maneira organizada profissionalmente com fins econômicos deve manter os respectivos registros de acesso à aplicações de internet pelo prazo de seis meses (BRASIL, 2014).

Quanto à requisição judicial dos registros de acesso pela parte, a Seção IV dispõe que:

> Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.
> Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
> I - fundados indícios da ocorrência do ilícito;
> II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
> III - período ao qual se referem os registros.
> Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro. (Brasil, 2014)

Há pesquisadores que consideram que esse prazo pode ser uma medida controversa, como Humberto de Oliveira Pedra dos Santos (2017): “Tal ferramenta é poderoso meio de combate aos crimes cibernéticos, talvez a maior de todas já

criada para tal finalidade no âmbito jurídico brasileiro. Entretanto tem caráter demasiado invasivo, podendo comprometer a privacidade dos usuários.”. Ou seja, seu potencial de violação da intimidade pode gerar certa tensão entre a eficácia e garantia dos direitos fundamentais.

Sobre a responsabilização dos provedores de conexão, a Lei nº 12.965/2014 dispõe que não haverá responsabilização civil pelos danos decorrentes de conteúdo gerados por usuários, exceto nos casos em que há ordem judicial específica para a retirada do conteúdo gerado por terceiros e o provedor não tomar as providências específicas.

É importante mencionar que os provedores de serviço podem, por meio de seus próprios termos de uso, estabelecer os requisitos para a remoção de conteúdos, permitindo assim o atendimento a notificações extrajudiciais enviadas por supostas vítimas de danos decorrentes de publicações específicas (LEMOS; SOUZA, 2016).

A escolha pelo regime de responsabilidade civil subjetiva justifica-se pelo entendimento de que a responsabilidade objetiva poderia levar os provedores a monitorarem excessivamente e a removerem conteúdos potencialmente polêmicos. Tal conduta configuraria uma restrição indevida à liberdade de expressão (TEFFÉ; MORAES, 2017). Além disso, o regime objetivo geraria incerteza sobre a responsabilidade do provedor, considerando que poderia se tornar um obstáculo ao desenvolvimento tecnológico, científico, cultural e social.

Exigiria, ainda, que o provedor exercesse controle prévio sobre todas as publicações, medida que poderia ser interpretada como censura e elevar os custos do serviço. Ademais, quanto à responsabilização civil quanto aos direitos autorais retratada no § 2º do artigo 19 (BRASIL, 2014), é pertinente afirmar:

> No Brasil, mesmo que não haja uma lei que regule especificamente o tema da responsabilidade civil por violação de conteúdo protegido por direito autoral, entidades e empresas de internet acabaram adotando o mecanismo conhecido como notice and take down ou notificação e retirada. Desta forma, os detentores de direitos autorais enviam uma notificação para a empresa, pedindo a remoção do conteúdo, e esta notifica a pessoa que postou o conteúdo. Se ela não assumir a responsabilidade pela veiculação do material, o provedor poderá remover o conteúdo. (Teffé; Moraes, 2017)

Quanto ao princípio da neutralidade da rede, disposto no artigo 9º do Marco Civil da Internet (2014): “Art. 9º O responsável pela transmissão, comutação ou

roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.”.

> A regra deve ser, portanto, o tratamento isonômico dos pacotes de dados, sem distinção por conteúdo, origem, destino, serviço, terminal ou aplicação, havendo expressa vedação ao bloqueio, monitoramento, filtragem ou análise do conteúdo dos pacotes (art. 9º do MCI). O princípio impõe que a filtragem ou os privilégios de tráfego devam respeitar apenas e tão somente critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos ou culturais que criem qualquer forma de discriminação ou favorecimento. (Teffé; Moraes, 2017)

2.2.3 Legislação penal brasileira relacionada aos crimes cibernéticos

Algumas das transgressões perpetradas no ambiente virtual já estão contidas na legislação penal brasileira, é válida a análise acerca dos crimes passíveis de adaptação para os meios virtuais. O crime de calúnia, contido no artigo 138 do Código Penal (1940), é um crime contra a honra que pode ser impulsionado pelo ambiente virtual.

No mesmo diploma normativo, consta o crime de difamação, que segundo o artigo 139, consiste em imputar a alguém fato ofensivo à sua reputação (BRASIL, 1940). Um exemplo de como isso pode se suceder no meio virtual seria um encaminhamento de e-mail para várias pessoas com boato acerca de um indivíduo.

No artigo 140 do Código Penal (BRASIL, 1940), há a determinação acerca do crime de injúria, que seria ofender ou insultar verbalmente, fisicamente ou por escrito ofendendo a dignidade ou decoro do indivíduo. Esse delito pode ser cometido através da internet em comentários de perfis de redes sociais que tenham como objetivo degradar ou insultar a imagem da vítima.

Entre as infrações cometidas no meio virtual, está o crime de divulgação de segredo, contido no artigo 153 do Código Penal (1940), que tem sua conduta pautada pela divulgação de documentos particulares ou correspondência confidencial, dados confidenciais ou protegidos de terceiros e cuja divulgação possa acarretar em dano para o usuário. O crime de dano, disposto no artigo 163 do Código Penal, trata sobre a destruição, inutilização e deterioração de patrimônio de terceiros, que pode ser realizado através da internet com o envio de vírus que

acarrete na destruição de equipamentos ou conteúdos armazenados nos dispositivos (BRASIL, 1940).

Em seu artigo 171, o Código estabelece que o crime de estelionato se dá através da obtenção de vantagem ilícita em prejuízo alheio mediante meio fraudulento que induza o sujeito a erro (BRASIL, 1940). Com a internet, os infratores passaram a dispor de diversos mecanismos para ludibriar as vítimas, simulando operações e vendas fraudulentas, se passando por empresas legítimas com sites clonados e realizando operações fraudulentas utilizando nomes de terceiros.

O peculato eletrônico, consoante o Código Penal Brasileiro, seria a inserção de dados falsos, alteração ou exclusão indevida dos dados constantes nos sistemas informatizados ou em bancos de dados da administração pública por funcionário autorizado com o objetivo de conseguir vantagem indevida para si ou para terceiros, ou causar dano (BRASIL, 1940). Paralelamente, o artigo 313-B trata sobre a alteração não autorizada em sistema de informações por funcionário público sem a anuência da autoridade competente (BRASIL, 1940). Os novos tipos penais foram adicionados ao Código Penal após a Lei nº 9.983 de 2000.

Entre os crimes mais reincidentes no ambiente virtual atualmente, está a pirataria de *software*, que não se restringe apenas à reprodução ou cópia dos programas, popularmente chamados de “piratas” (SANTOS, 2017). A Lei nº 9.609 de 1998 tipifica o delito a partir da reprodução, por qualquer meio, de programa de computador para fins comerciais sem que haja aprovação do autor ou representante.

A pena é igualmente aplicável nos casos em que o autor vende, divulga, importa no País, oculta ou mantém em depósito para fins comerciais as réplicas dos programas confeccionadas com violação de direito autoral.

2.2.4 Lei Carolina Dieckmann

Uma importante legislação no que diz respeito aos delitos virtuais é a Lei nº 12.737 de 2012, conhecida de forma popular como Lei Carolina Dieckmann, quando a atriz sofreu com o vazamento de fotos íntimas armazenadas em seu computador após extorsão (SANTOS, 2017). O fato ocorreu no dia 6 de maio de 2012, ocasião em que o jornal O Estado de S. Paulo publicou que fotos íntimas da atriz Carolina Dieckmann haviam sido divulgadas, rapidamente se tornando um dos temas mais comentados no *Twitter* (VALLE, 2012; BELINOTTE *et al.* 2024).

Ao longo das semanas seguintes, o episódio continuou a repercutir em diversas reportagens de jornais e na televisão. Em 14 de maio de 2012, os responsáveis foram localizados por meio do rastreamento de seus endereços IP (VALLE, 2012). Foi constatado então que as imagens haviam sido obtidas diretamente do e-mail da atriz e que os suspeitos tentaram extorqui-la, exigindo pagamento para não torná-las públicas (BELINOTTE *et al.* 2024).

A lei dispõe acerca desse tipo de situação, tipificando o delito de invasão de dispositivo informático em seu artigo 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. (Brasil, 2012)

Referente ao artigo em questão, é pertinente destacar:

> Frisa-se o caput desse artigo foi acertadamente formulado, punindo um tipo de crime onde o bem jurídico a ser protegido é o sistema de computadores em si. Depreende-se da leitura deste artigo também que o delito só ocorre quando o indivíduo tem o **dolo** de cometer a ação, como está expresso ao dizer "(...) com **o fim** de obter, adulterar ou destruir dados ou informações (...)" (GRIFO NOSSO), não sendo cabível neste tipo penal a modalidade culposa de conduta. Logo, o usuário que inadvertidamente compartilha ou encaminha *malwares* não está cometendo crime algum. (Santos, 2017)

A norma atenta também para os indivíduos que produzem, oferecem, distribuem, vendem ou difundem programas e dispositivos capazes de permitir a prática desse crime, com aumento da pena se gera prejuízo econômico e resulta obtenção de informações e conteúdos sigilosos, segredos comerciais e comunicações eletrônicas privadas (BRASIL, 2012).

> Aqui cabe a ressalva de que ainda não está pacificado nos tribunais o que é necessário que ocorra para caracterizar a violação indevida de mecanismo de segurança, conforme é definido no dispositivo legal, visto que nem sempre o usuário possui qualquer nível de segurança implementado ou que talvez seja inviável comprovar tal violação. (Caiado; Caiado, 2018)

É perceptível, ainda sobre o artigo supracitado, em seu § 3º, a seguinte referência quanto ao controle de forma remota e não autorizada do dispositivo:

> aos *botnets*, *malwares* que infectam computadores sem os próprios usuários perceberem, transformando seus dispositivos em “zumbis” que realizam determinada ação orquestrada pelo cibercriminoso muitas vezes sem o conhecimento ou consentimento dos proprietários dos computadores infectados. (Santos, 2017)

Nesses crimes, consoante os pressupostos legais, a ação penal é procedida apenas por meio de representação, exceto nos casos em que o crime é cometido contra a administração pública direta ou indireta de qualquer dos poderes dos entes da federação ou contra empresas concessionárias de serviços públicos (BRASIL, 2012). Ademais, houve modificação de outros artigos do Código Penal, como o artigo 266, que trata sobre a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.

A adição faz constar que o indivíduo que interromper, impedir ou dificultar o serviço ou restabelecimento do serviço telemático ou de informação sofrerá as mesmas penas destinadas aos casos citados no diploma normativo anterior, além da aplicação em dobro da pena nos casos em que o crime é cometido por ocasião de calamidade pública (BRASIL, 2012).

Do mesmo modo, houve atualização no artigo 298 do Código Penal Brasileiro, que em seu parágrafo único equiparou os cartões de crédito e débito aos documentos particulares que são citados na norma de falsificação de documento particular (BRASIL, 2012).

2.2.5 Legislação Geral de Proteção de Dados (LGPD)

A Legislação Geral de Proteção de Dados (LGPD) constitui pressupostos para tratamento de dados pessoais nos meios digitais, visando proteger a privacidade e o livre desenvolvimento da pessoa natural através de ações da pessoa natural ou jurídica de direito público ou privado (BRASIL, 2018).

> A LGPD tornou-se a principal fonte legislativa do ciberespaço brasileiro, apesar de não estabelecer especificamente a regulamentação de segurança cibernética. A LGPD estabeleceu a Agência Nacional de Proteção de Dados como ator central na imposição de sanções administrativas e na regulação de parâmetros sobre a temática. (Belinotte *et al.*, 2024)

A LGPD apresenta seus principais fundamentos já no artigo 2°:

> I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (Brasil, 2018)

A LGPD estabelece diretrizes sobre a forma como as empresas devem administrar as informações pessoais dos consumidores, definindo em quais circunstâncias esses dados podem ser considerados sigilosos, se é permitida ou não sua comercialização e quais procedimentos devem ser observados em seu tratamento. Embora possua um escopo abrangente, a norma também suscita debates acerca de eventuais excessos de controle estatal e de potenciais riscos às liberdades individuais e coletivas (BELINOTTE *et. al*, 2024).

Não obstante, cabe destacar que:

> A utilização das redes sociais virtuais modificou profundamente a forma de obtenção, tratamento e divulgação de dados pessoais, o que impactou diretamente a própria expectativa de privacidade da pessoa humana. Nos dias atuais, dificilmente o indivíduo poderá alcançar um alto grau de controle sobre as suas informações e características pessoais depois que as inserir na rede. Dessa forma, pode-se afirmar que a velocidade da circulação da informação é inversamente proporcional à capacidade de seu controle, retificação e eliminação. (Teffé; Moraes, 2017)

A lei determina como requisitos para o tratamento de dados o consentimento do titular, a finalidade de cumprimento de obrigação legal regulatória, a necessidade compartilhamento de dados para a execução de políticas públicas pela administração pública e quando imprescindível para execução de contrato ou procedimentos que possuam relação com o contrato que o titular faça parte (BRASIL, 2018).

A realização de estudos por órgão de pesquisa, feito o tratamento e anonimização dos dados também permite o tratamento dos dados pessoais, assim como o exercício regular de direitos em processo judicial, administrativo ou arbitral e proteção da vida do usuário (BRASIL, 2018). Entre o rol contido no artigo 7° da LGPD, está a finalidade de proteção do crédito e a tutela da saúde em procedimentos desempenhados por autoridade sanitária (BRASIL, 2018).

Quanto ao consentimento do usuário, deve conter de forma expressa a finalidade do tratamento dos dados pessoais e pode ser revogado a qualquer

momento pela manifestação expressa do titular mediante um procedimento gratuito e facilitado (BRASIL, 2018). Além disso, o ônus da prova que houve consentimento conforme o artigo é da parte responsável pelo controle e tratamento de dados (BRASIL, 2018).

No que diz respeito ao tratamento de dados pessoais de crianças e adolescentes, há a exigência de consentimento específico por pelo menos um dos pais ou responsável legal, exceto quando as informações coletadas forem necessárias para contatar os pais ou responsável legal, mas desde que os dados sejam utilizados uma vez, não sejam repassados a terceiros ou armazenados (BRASIL, 2018).

Entre os direitos do titular dos dados, está a confirmação quanto à existência de tratamento, acesso e correção de dados incompletos ou desatualizados, tratamento anônimo, bloqueio ou eliminação de dados sem necessidade e excessivos, bem como portabilidade dos dados para outro fornecedor de serviço ou produto e informação sobre as entidades com as quais houve o compartilhamento de dados (BRASIL, 2018).

2.3 Dificuldades de implementação de políticas regulatórias no ciberespaço

2.3.1 Barreiras para o aplicador do Direito

O descompasso entre a eclosão de novas tecnologias, relacionamentos interpessoais no ciberespaço e os sistemas legais, gera novas ameaças e vulnerabilidades para o usuário da rede mundial de computadores e para o aplicador do Direito, que precisa estar cada vez mais atento à pluralidade de ferramentas.

Entre os empecilhos, a investigação e a punição de crimes praticados por suspeitos localizados em outros países apresentam consideráveis obstáculos, o que contribui para a percepção de impunidade e para a formação da ideia de que o ciberespaço configura uma terra sem lei (BELINOTTE *et. al*, 2024). Esse cenário favorece a atuação de agentes envolvidos em práticas ilícitas no ambiente virtual e, simultaneamente, intensifica a sensação de insegurança entre os cidadãos, sobretudo entre aqueles com menor familiaridade com os recursos tecnológicos (BELINOTTE *et. al*, 2024).

Com a imaterialidade do ciberespaço, os infratores conseguem gerar inúmeros danos em qualquer lugar do planeta (CONTE; SANTOS, 2008), tornando a competência para investigação e julgamento desses casos uma questão delicada. Essa realidade virtual gera impactos reais especialmente no cotidiano dos brasileiros, tendo em vista que o país possui um dos maiores índices mundiais de usuários conectados à internet consoante dados extraídos de pesquisa disponibilizada pela *Our World Data* (RITCHIE *et al.*, 2023), apresentando uma taxa de 84,2 % da população conectada à internet.

Nesse contexto, é relevante falar sobre o conceito de *Internet Protocol*, ou IP, que se trata de um número recebido por cada dispositivo que se conecta com a internet e é registrado a partir de cada acesso aos serviços informatizados (BRASIL, 2014). Esse endereço é o que torna possível a identificação do terminal de uma rede, desde que o equipamento tenha estabelecido conexão com a internet (BRASIL, 2014).

Com o avanço da capacidade investigativa dos operadores do Direito, os infratores passaram a especializar cada vez mais suas práticas para gerar mais entraves nos processos de investigação e apuração de informações, adotando formas de proteger e mascarar o IP, como o uso das redes privadas virtuais (VPNs) (SANTOS, 2017). Assim, nem sempre é possível utilizar o IP como identificação e meio de localização dos autores dos cibercrimes.

Além disso, para que as autoridades acessem o *Internet Protocol* dos usuários, é necessária uma autorização judicial (BRASIL, 2014), visto que a necessidade de proteção dos usuários não pode prejudicar o direito à liberdade e à vida privada. Com o IP, o operador consegue não apenas localizar de onde partiu a comunicação do usuário, mas também seu endereço e outros dados cadastrais (SANTOS, 2017).

Essa busca depende de requisição partindo de membro do Ministério Público ou Delegado de Polícia, considerando a necessidade de cautela para que não sejam violados pressupostos fundamentais (SANTOS, 2017; BRASIL, 2014).

> A questão de obter o IP sem autorização judicial é problemática por vários motivos. Caso o usuário não mascare seu IP, é possível saber exatamente de qual computador partiu a comunicação, seja ela um post no Facebook, um vídeo postado no Youtube ou até mesmo um simples comentário num blog. (Santos, 2017)

Para que os profissionais consigam combater de modo efetivo os cibercrimes, é necessário conscientizar os usuários de internet ao passo que se especializam, configurando esse o método mais eficaz para a prevenção da prática desses delitos (SANTOS, 2017).

Outro desafio no que diz respeito à investigação de crimes cibernéticos é a complexidade das provas digitais, já que em muitos casos há o prejuízo da evidência pela falta de procedimentos estabelecidos que se adequem à coleta de provas. Diante disso, é propagada uma sensação de insegurança, tanto dentro no nosso próprio corpo quanto para determinar o local do crime.

Ao falar sobre os limites entre a privacidade dos usuários, censura e enfrentamento da criminalidade virtual, é válido citar Cassanti (2014):

> Remoção de conteúdo: Segundo o Marco Civil, os provedores de conexão à internet não serão civilmente responsáveis por danos relacionados ao conteúdo gerado por terceiros (essas empresa não responderão na Justiça pelo conteúdo publicado por seus usuários. Isso só acontecerá, após ordem judicial, a empresa não tome as providências para tornar o conteúdo indisponível. Dados pessoais: O Marco Civil assegura ao internauta o direito ao sigilo de suas comunicações via internet (salvo por ordem judicial); informações claras e completas dos contratos de prestação de serviço; não fornecimento a terceiros de seus registros (...) Neutralidade da rede: Este item propõe que o responsável pela transmissão do conteúdo deve tratar de forma igual quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino. É a chamada neutralidade da rede.

A partir disso, verifica-se que o Marco Civil da Internet, ainda que tenha buscado consolidar a proteção dos direitos dos usuários no ambiente digital, revela-se insuficiente ao tentar estender instrumentos jurídicos tradicionais a um cenário virtual marcado por dinamismo acelerado e complexidade crescente (SANTOS; SOTERO, 2024).

Essa constatação evidencia, de forma contundente, a urgência de uma revisão legislativa que seja capaz de responder com maior eficácia aos desafios impostos pelos crimes cibernéticos, promovendo uma inovação no que diz respeito às normas que dialoguem de maneira consistente com as exigências e peculiaridades da sociedade digital contemporânea (SANTOS; SOTERO, 2024).

É importante frisar que a legislação corrente acerca do tratamento e segurança de dados, como a LGPD, é um potente instrumento para o operador do direito, já que prevê sanções em casos de vazamento de dados e quebra de

privacidade (BRASIL, 2018). Não obstante, esse diploma normativo ainda está em processo de solidificação, promovendo mudanças nas empresas brasileiras para uma adaptação ao novo processo de tratamento de dados e proteção dos usuários no ambiente digital (SANTOS; SOTERO, 2024).

O fortalecimento das leis, aliado à capacitação dos profissionais para investigar os crimes digitais e aplicar integralmente as normas existentes é imprescindível para conter as infrações (MEIRELES; PASITTO, 2024). A despeito das dificuldades retratadas, o Brasil é um dos países com maior arsenal legislativo em relação à legislação que disciplina o ciberespaço, consoante o Relatório de Cibersegurança Global (RCG) referente ao ano de 2020, o Brasil teve nota máxima direcionada às medidas legais direcionadas para a segurança cibernética entre os países em desenvolvimento (ITU, 2021)

No entanto, a existência de uma estrutura robusta legislativa não consegue garantir, por si só, a efetividade no enfrentamento aos crimes digitais. A distância entre as normas e a realidade prática destacam que, além da elaboração das leis, é preciso investir nos mecanismos de aplicação e modernização dos órgãos investigativos, além da busca pela cooperação internacional.

2.3.2 Jurisdição da internet

O ciberespaço não possui fronteiras, delimitações territoriais e barreiras físicas, multiplicando as relações humanas e tornando mais complexas as investigações de delitos que deixaram provas digitais (DOMINGOS; RÖDER, 2018). Ao tratar anteriormente sobre o as aplicações de internet e o número IP (*Internet Protocol)*, foi possível depreender que:

> O funcionamento correto dessa rede obedece a critérios organizacionais matemáticos, que permitem a fluidez dessa estrutura. Isso significa que as empresas provedoras de internet detêm as informações referentes aos passos que os usuários percorrem na rede: acessos, postagens e comunicações. São essas informações que em geral permitem, de forma precisa, desvendar um crime cibernético ou obter uma prova digital para elucidar um crime real. O que tem aturdido o mundo jurídico é a obtenção dessas informações, desses dados que consubstanciam a prova digital. (Domingos; Röder, 2018)

A obrigação de as empresas manterem volumosos conjuntos de dados, seja por exigências de *compliance* e gestão interna, seja em decorrência das normas

jurídicas às quais se submetem, tem conduzido ao armazenamento dessas informações em servidores distribuídos em diversos países, segundo critérios de ordem econômica e fiscal (DOMINGOS; RÖDER, 2018).

> Principalmente quando se constata que a dinâmica fluida das condutas delituosas cometidas na web e a dificuldade de definição da jurisdição aplicável tornam mais difícil o combate à cibercriminalidade. A harmonização entre o Direito Internacional, seus instrumentos jurídicos como Declarações, Convenções, Acordos multilaterais ou bilaterais, e as legislações internas dos diferentes Estados nacionais passa a ser elemento essencial para a efetividade desse combate. (Santos, 2018)

Além disso, como medida de segurança e de continuidade operacional, há a replicação de servidores em diferentes territórios, visando a fragmentação e o armazenamento descentralizado de dados, prática que levanta questões relevantes em torno da soberania informacional e da determinação da jurisdição aplicável (DOMINGOS, RÖDER, 2018). Considerando esse cenário que anteriormente haviam os Acordos de Assistência Mútua em Matéria Penal, ou *Mutual Legal Agreement Treaties* (MLATs), os quais eram traduzidos e encaminhados pelas autoridades para a execução do pedido após análise por outra autoridade no país requerido (DOMINGOS; RÖDER, 2018).

Considerando o caráter impermanente das provas digitais, esse procedimento mais tradicional caiu em desuso, atualmente o que ocorre é que os operadores do Direito realizam a ponte direta com as empresas provedoras de internet, principalmente nas situações em que há vínculo da empresa como local que foi impactado pela ação delituosa onde o crime está sob investigação (DOMINGOS; RÖDER, 2018).

Foi verificado anteriormente que a Convenção de Budapeste (BRASIL, 2023) estabelece um prazo para conservação de dados e obtenção de provas digitais, assim como auxílio mútuo para fornecimento de dados de tráfego e interceptação dos conteúdos (DOMINGOS; RÖDER, 2018). Sobre os dados armazenados fora do território de cada Estado, não soluciona integralmente a questão:

> Art. 32. Acesso transfronteiríço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público
> Uma Parte pode, sem autorização de outra Parte: a) Aceder a dados informáticos armazenados acessíveis ao público (fonte aberta), seja qual for a localização geográfica desses dados; ou
> b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra

> Parte, se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados, através deste sistema informático. (Brasil, 2023)

Quanto à aplicação do Código Penal Brasileiro, continua sendo adotado o Princípio da Ubiquidade, disposto no artigo 6º do diploma normativo (BRASIL, 1940), ou seja: "Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.". À vista disso, quando o crime cibernético ocorre no país, o autor está sujeito à jurisdição brasileira e é dever do Estado realizar a investigação para apurar o delito.

2.3.3 O agente infiltrado virtual como nova ferramenta de investigação

Averiguando a disposição normativa de vários países, é possível observa um consenso sobre a figura do agente infiltrado, geralmente há a infiltração em uma rede de delinquentes, ocultação da sua verdadeira identidade e, em alguns países, a condição de agente estatal do indivíduo (BUFFON, 2018). No Brasil, anteriormente eram aplicáveis atuações desse tipo apenas para questões relacionadas à quadrilha, associação ou organização criminosa relativa a entorpecentes, como a Lei nº 11.343/2006 (BUFFON, 2018).

Com a Lei nº 12.850 (BRASIL, 2013), houve o acréscimo de novos crimes na ferramenta para busca de autoria e materialidade delitiva, permitindo a realização de investigações no mundo virtual. Desde que exista representação do delegado de polícia ou requerimento do Ministério público, após manifestação técnica do delegado quando solicitada no curso do inquérito policial, será possível a infiltração de agente de polícia em tarefas de investigação. No que tange à infiltração virtual:

> Art. 10-A. Será admitida a ação de agentes de polícia infiltrados virtuais, obedecidos os requisitos do caput do art. 10, na internet, com o fim de investigar os crimes previstos nesta Lei e a eles conexos, praticados por organizações criminosas, desde que demonstrada sua necessidade e indicados o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas. (Brasil, 2013)

Conforme o artigo 12 do diploma normativo supracitado, a solicitação de infiltração será distribuída de forma sigilosa, não sendo revelada a identificação do agente (BRASIL, 2013).

> Para o agente infiltrado obter a identificação de autoria e materialidade dos usuários delinquentes, possivelmente será necessário um tempo considerável, a fim de, em momento posterior, serem executados mandados de busca e apreensão, preferencialmente, no mesmo dia em todo país, não frustrando o trabalho, já que a comunicação na internet é instantânea e pode gerar comprometimento em obter a mídia que irá fortalecer a prova dos crimes detectados. (Buffon, 2018)

Com isso, a ação controlada pode ser autorizada pelo prazo de até seis meses, se prejuízo de eventuais renovações por meio de ordem fundamentada pela autoridade judicial (BRASIL, 2013). É relevante, ainda, destacar a diferença entre agente infiltrado e agende provocador.

Dentre as características do agente infiltrado, estão:

> - **objetiva coletar informações** – a observação de um ambiente fechado virtual é essencial para a busca de dados que podem esclarecer ou identificar autoria e/ou materialidade delitiva. A análise de relações entre pessoas e/ou empresas pode ser essencial para o esclarecimento de crimes que usam o meio digital como fim ou como meio para realização de seus fins;
> - **postura passiva** – a ação do agente infiltrado não terá o objetivo de levar o investigado a cometer crimes. Exatamente o oposto. No entanto, importante se ter bem presente que isso não exclui a possibilidade de esse mesmo agente estatal cometer algum ato que se caracterize infração penal, mas tão somente nos limites estabelecidos na decisão judicial;
> - **obtém a confiança do suspeito** – os criminosos possuem muita cautela para permitir o ingresso de um novo integrante em suas redes fechadas. O receio de que seja um investigador faz parte dessa precaução. Decorre, assim, a necessidade de o agente infiltrado ter de ultrapassar tal limite para que possa fazer parte daquele círculo, a fim de coletar as informações necessárias.
> - **possui participação acessória** – como dito acima, o domínio do fato criminoso é uma atividade exclusiva do delinquente. O agente infiltrado deve estar atento às suas funções no ambiente que examina, colhendo as provas e agindo exatamente nos ditames dispostos pelo Juízo. (Buffon, 2018)

Já o agente provocador, diferente do agente infiltrado, tem impacto na impossibilidade da consumação do delito, instigando a execução do crime e prejudicando na identificação da motivação do infrator, de maneira oposta do resultado obtido pelo agente infiltrado, que busca não interferir na prática do crime (BUFFON, 2018). Outrossim, o agente provocador também possui domínio final do fato, sendo imprescindível para a execução do crime (BUFFON, 2018).

No contexto digital, uma ampla variedade de condutas ilícitas demanda identificação e apuração minuciosa. Nesse sentido, tanto redes de acesso público quanto ambientes restritos devem ser examinados, a fim de assegurar a correta

determinação da materialidade e da autoria dos delitos, podendo-se ainda recorrer a estratégias investigativas complementares.

Cumpre destacar, no entanto, que cada espaço virtual apresenta particularidades específicas, que necessitam ser consideradas para a obtenção de autorização judicial, sempre em conformidade com os princípios da proporcionalidade e da necessidade, garantindo, assim, a legalidade e validade das provas coletadas.

2.3.4 Projeto "Ministério Público pela Educação Digital nas Escolas"

O projeto em questão tem como objetivo a realização de oficinas por todo o país conscientizando educadores, crianças e adolescentes sobre o mundo virtual, é coordenado pela Procuradoria Federal dos Direitos do Cidadão (PFDC), através do Grupo de Trabalho Comunicação Social, com auxílio do Grupo de Apoio no Combate aos Crimes Cibernéticos (2ª Câmara de Coordenação e Revisão do MPF) e do Grupo de Trabalho Tecnologia da Informação e Comunicação (3ª Câmara de Coordenação e Revisão do MPF).

> O projeto "Ministério Público pela Educação Digital nas Escolas" se alinha às diretrizes estabelecidas pela Lei nº 12.965/2014 – também conhecida como Marco Civil da Internet – que, em seu art. 26 destaca o dever constitucional do Estado na prestação da educação para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da, para a promoção da cultura e para o desenvolvimento tecnológico. (Oliveira; Morgado, 2018; Brasil, 2014)

Em reuniões que abordam temas como *ciberbullying, sexting*, uso excessivo das redes e aliciamento de menores, são desenvolvidas atividades pedagógicas no que trata do uso consciente da rede mundial de computadores (OLIVEIRA; MORGADO, 2018). Acerca de sua organização:

> A oficina é agendada, em regra, pelo procurador regional dos Direitos do Cidadão23 da capital do estado, em reunião prévia com as Secretarias Municipais e Estaduais de Educação e de Assistência Social, os Institutos Federais de Ensino e o Sindicato das Escolas Privadas e tem, por dinâmica, o seguinte formato: na parte da manhã, iniciam-se os trabalhos com uma palestra do procurador da República que organiza a oficina na sua cidade, na qual é explicado aos presentes o papel do Ministério Público relacionado ao tema, seja no âmbito criminal, seja no âmbito da cidadania. Em seguida, o psicólogo e educador da ONG SaferNet, Rodrigo Nejm, inicia a capacitação dos educadores, demonstrando os mais diversos tipos de

> violações aos direitos humanos que ocorrem no mundo virtual e dos quais as crianças e os adolescentes podem ser vítimas ou agentes. Na parte da tarde, em continuação, são distribuídos materiais pedagógicos (cartilhas, cartazes e folders didáticos) para a introdução do assunto em sala de aula. É oportunizado tempo para perguntas pelos participantes e para a discussão de situações práticas, cada vez mais vivenciadas no ambiente escolar, bem como são demonstrados os meios existentes para o adequado encaminhamento às autoridades das notícias de crimes que venham a ter conhecimento. (Oliveira; Morgado, 2018)

Com esse estímulo para as crianças e adolescentes, é possível tratar sobre o potencial da rede, mas ainda adequando os diálogos ao público (OLIVEIRA; MORGADO, 2018).

> O acesso rápido e com dispositivos móveis à internet introduziu novas formas de relacionamento entre as pessoas. Ao mesmo tempo em que o cenário tecnológico afastou fisicamente os seres humanos, ele acabou por proporcionar contato frequente, direto e interativo entre eles, gerando uma nova forma de convivência. Inverteu-se a antiga regra de que primeiro seria necessário um contato físico para que só então fosse possível chegar à comunhão de ideias. Em tempo real, indivíduos e grupos participam ativamente da construção, discussão e seleção das informações que serão inseridas na rede. (Teffé; Moraes, 2017)

Nos últimos anos, tem-se observado uma utilização cada vez mais intensa, sobretudo por parte dos jovens, de diversas ferramentas digitais destinadas à divulgação de aspectos de suas vidas privadas sem a devida conscientização ou vigilância. Tanto os acontecimentos de maior relevância quanto os elementos de menor significado vêm sendo amplamente compartilhados em redes sociais e aplicativos interativos sem maiores critérios quanto ao público ou atenção ao conteúdo, que pode ser utilizado pelos cibercriminosos tanto para extrair informações sensíveis, quanto para reprodução em sites voltados para pedofilia.

> Nos últimos anos, lesões à privacidade, à honra, ao nome e à imagem da pessoa humana vêm ocorrendo de forma exponencial, tendo o ambiente virtual como o principal meio. Verifica-se que as diversas oportunidades que as redes sociais virtuais oferecem aos seus usuários, atreladas à extrema facilidade para a criação de contas pessoais, grupos e postagens, acabam contribuindo para a usurpação e a exposição injustificada de direitos de terceiros. Perfis falsos, descrições difamatórias e a exibição não consensual de imagens e informações íntimas são exemplos de utilização desses canais de comunicação que geram graves danos à pessoa humana. (Teffé; Moraes, 2017)

Essa atuação conjunta, buscando integração com as gerações futuras e conscientização quanto aos equipamentos com acesso à internet é uma importante

iniciativa no combate aos crimes cibernéticos, disponibilizando tempo para esclarecer dúvidas e difundindo esclarecimento sobre esse ambiente tão vasto como o ciberespaço.

De acordo com Neide Oliveira e Márcia Morgado (2018):

> Desde o ano de 2015, foram realizadas mais de 20 (vinte) oficinas, no Distrito Federal e nos seguintes estados: Amazonas, Bahia, Ceará, Espírito Santo, Mato Grosso, Minas Gerais (duas vezes), Pará, Paraíba, Pernambuco, Rio de Janeiro (duas vezes), Rio Grande do Sul, Rondônia, Santa Catarina, São Paulo (para comunidades indígenas também, a pedido da Funai local), Tocantins e Mato Grosso do Sul, tendo-se por meta alcançar os demais estados até o final do ano 2017, o que de fato, ocorreu, com a realização da última oficina, na cidade de Natal, no mês de dezembro de 2017.

O objetivo central do projeto é unir esforços na prevenção e no enfrentamento da pornografia infantil, do racismo e de outras formas de discriminação presentes na internet. Para alcançar esse objetivo, o Ministério Público Federal conta com a parceria da ONG SaferNet Brasil e com o apoio do Comitê Gestor da Internet no Brasil (OLIVEIRA; MORGADO, 2018). A iniciativa busca capacitar professores das redes pública e privada de ensino fundamental e médio para que orientem seus alunos quanto ao uso saudável e responsável da internet, ensinando-os a se proteger de criminosos e a evitar comportamentos que possam levá-los a se tornarem futuros agressores (OLIVEIRA; MORGADO, 2018).

Para uma maior efetividade das normas penais, há uma necessidade de cooperação:

> Há necessidade de estratégias que envolvam políticas públicas bem elaboradas para prevenir a ocorrência do delito, para punir o autor do delito, tratar o delinquente, dar apoio e proteção às vítimas, e criar mecanismos de cooperação internacional (jurídica, policial etc.) entre Estados e organizações internacionais públicas e privadas. O combate à cibercriminalidade precisa seguir uma “macropolítica” que interconecte esse conjunto de aspectos, sem o que esse combate estará fadado ao insucesso. (Santos, 2018).

3 Considerações finais

No presente trabalho, após a análise dos principais conceitos relativos ao ambiente virtual, suas ameaças e vulnerabilidades, assim como os conceitos apresentados na legislação brasileira e por parte de doutrinadores, foi possível

observar a complexidade dos crimes cibernéticos e suas diversas formas de enfrentamento.

A princípio, em seu primeiro capítulo, foi examinado o conceito de crime em geral, afunilando posteriormente e adequando a discussão ao contexto dos crimes cibernéticos, aplicando a teoria tripartite aos crimes puros, impuros e mistos. Além disso, ao tratar dos crimes cibernéticos, foram analisadas principalmente as figuras dos *hackers* e *crackers*, que sujeitos em evidência no ciberespaço.

Quanto às principais ameaças no ambiente virtual, observa-se que há uma grande variedade de *malwares*, que evoluíram de forma sofisticada com o objetivo de explorar cada vez mais as vulnerabilidades dos dispositivos e ingenuidade dos usuários. Com a conceituação dos vírus, *worms*, *botnets, ransomwares* e cavalos de Troia, assim como exemplificação, foram demonstradas algumas estratégias utilizadas pelos infratores cibernéticos, objetivando uma maior elucidação e conscientização sobre a possibilidade de comprometimento silenciosa de um sistema de informática.

Por meio do entendimento quanto ao funcionamento e gatilho desses mecanismos, aliado às possíveis implicações jurídicas e sociais, foi adotada uma abordagem multifatorial para a promoção de um ambiente digital mais seguro com mitigação dos riscos.

Partindo da análise das legislações nacionais e internacionais no que tange aos crimes cibernéticos, foi evidenciado que o Brasil possui firme arcabouço jurídico, apesar de ainda apresentar constante necessidade de adaptação ás transformações da tecnologia. Quanto à Convenção de Budapeste, é notória sua importância para a cooperação internacional contra os crimes cibernéticos, fornecendo base para a legislação acerca do ciberespaço de maneira padrão.

O estudo do Código Penal e sua aplicabilidade aos delitos cometidos na internet foi importante para verificar de quais maneiras seria possível aplicar o diploma normativo e sua flexibilidade e adaptação frente à novas demandas sociais, assim como seu limite no tocante ao ambiente da inovação tecnológica. Algumas condutas mais refinadas pelos criminosos necessitaram de novos dispositivos legais para uma tipificação e direcionamento mais adequados, preservando a essência da conduta.

Paralelamente, o Marco Civil da Internet foi fundamental para consolidar direitos e regulamentar o uso da internet no país, evidenciando a importância da

privacidade, liberdade de expressão e neutralidade quanto ao tratamento dos usuários na rede mundial de computadores. É possível compreendê-lo como uma “Constituição da internet”, já que possui direitos e deveres entre seu pressupostos definidos, pretendendo promover também a neutralidade de rede para evitar práticas abusivas.

Um ponto importante foi relativo aos prazos de armazenamentos de registros pelos provedores, que pode ser visto como um risco de monitoramento excessivo e indevido. Partindo do estudo de leis específicas, como a intitulada em homenagem à atriz Carolina Dieckmann, foi possível notar a relevância de respostas jurídicas rápidas adaptadas às novas ameaças e vulnerabilidades dos indivíduos no ambiente virtual para o combate das novas modalidades engendradas por parte dos infratores.

Além disso, ao realizar o estudo a respeito da Lei Geral de Proteção de Dados (LGPD) e o paradigma de proteção dos direitos fundamentais frente aos dados pessoais, foi constatado o desafio do aplicador do direito no papel de adotar certas medidas para empresas ainda despreparadas de pequeno e médio porte, assim como harmonização com as demais normas reguladoras. Ficou cristalino como cada um desses instrumentos desempenha um papel complementar no combate às vulnerabilidades virtuais.

Quanto às dificuldades enfrentadas pelo aplicador do direito na implementação de políticas regulatórias no ciberespaço, é indiscutível que a principal delas é o caráter volátil quanto aos crimes virtuais, que são de difícil localização e investigação. O crescimento desproporcional das especializações tecnológicas e estrutura dos dispositivos gera cada ver mais pontos vulneráveis a serem tratados pelo legislador brasileiro.

O refinamento das técnicas de proteção da identidade, mascaramento do endereço IP, necessidade de autorização para obtenção de dados em investigação e a sensação de insegurança no ciberespaço evidenciam uma necessidade delicada de equilíbrio entre a eficiência investigativa e abordagem adequada do aplicador do direito. Esse fator reforça a carência de capacitação especializada dos profissionais e conscientização dos usuários.

Acerca da jurisdição sobre crimes cibernéticos, a principal adversidade se dá pela sua transcendência, tanto entre servidores, dados e sistemas de armazenamento, quanto entre fronteiras físicas, considerando a possibilidade de um delito virtual em um determinado país gerar consequências em todo o globo. No que

tange à legislação penal brasileira, é possível aplicar o tradicional Princípio da Ubiquidade, já em instrumentos normativos como a Convenção de Budapeste, é encontrada uma natureza fundada na cooperação entre países.

É imprescindível pontuar que todos esses mecanismos de combate dependem do relacionamento entre autoridades, provedores de serviços e tratados internacionais com necessidade contínua de atualização. Foi pertinente explorar, no campo do direito penal brasileiro, a figura do agente infiltrado virtual, uma importante peça na apuração de crimes praticados por organizações criminosas no ciberespaço ou por intermédio dele.

Foram dispostas algumas condições no tocante a atuação desses agentes conforme a previsão legal, abordando seu caráter controlado, sigiloso e alguns procedimentos para que a não ocorra atuação fora do estabelecido e requerido não só pela lei, mas também fiel à investigação e solicitação do delegado de polícia e Ministério Público.

Foi destinado um tópico para a pornografia infantil, sua tipificação pelo Estatuto da Criança e do Adolescente (ECA), modalidades típicas de conduta e os obstáculos significativos, para combater esse crime, como a dificuldade em distinguir adolescentes de adultos em determinados arquivos, sobretudo em materiais de baixa resolução, além da utilização de redes P2P e da constante adulteração de conteúdos para escapar dos sistemas de *hash*.

Paralelamente ao aparato repressivo, destaca-se a importância de iniciativas preventivas, entre as quais se insere o projeto “Ministério Público pela Educação Digital nas Escolas”, coordenado pela Procuradoria Federal dos Direitos do Cidadão (PFDC), em parceria com a ONG SaferNet Brasil e com o Comitê Gestor da Internet no Brasil. Essa atuação preventiva paralela às diretrizes do Marco Civil da Internet, estabelece como dever do Estado fomentar a educação digital para o exercício da cidadania.

Assim, ao passo em que reforça a repressão penal, o projeto busca formar multiplicadores dentro do ambiente escolar, preparando os jovens para reconhecer riscos, adotar medidas de autoproteção e evitar comportamentos que possam acarretar em condutas criminosas. Com isso, é verificado que o enfrentamento da pornografia infantil requer uma abordagem integrada, combinando estratégias jurídicas, tecnológicas e educacionais.

A repressão, por meio do aperfeiçoamento investigativo, precisa caminhar lado a lado com a conscientização social, de modo a reduzir a vulnerabilidade de crianças e adolescentes. Com isso, é necessário reforçar a importância de meios investigativos modernos que consigam lidar com a complexidade das interações virtuais, harmonizando tecnologia, legislação e educação. A partir disso, é viável que seja alcançado um *status* mais proporcional de resposta para as crescentes ameaças atreladas às novas tecnologias e, consequentemente, ao ciberespaço.

Referências

BELINOTTE, Mariana Grilli; GOLDONI, Luiz Rogério Franco; DEVANNY, Joe; COELHO, Carlos Frederico. **Ordem e progresso? Analisando as respostas brasileiras aos cibercrimes.** Relações Internacionais, n. 82, junho 2024. Disponível em: https://ipri.unl.pt/images/publicacoes/revista_ri/pdf/ri82/RI_82_NET_MarianaBelinotte_et_al.pdf. Acesso em: 04 jan. 2025.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Publicado em: 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 10 out. 2024.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023.** Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Diário Oficial da União: seção 1, Brasília, DF, 13 abr. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 12 out. 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. Diário Oficial da União, Brasília, DF, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 23 out. 2024.

BRASIL. **Lei nº 12.850, de 2 de agosto de 2013.** Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Diário Oficial da União, Seção 1, Ed. Extra, Brasília, DF, 5 ago. 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 22 jan. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Seção 1, Brasília, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 out. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 4 jan. 2025.

BRASIL. **Lei nº 9.609, de 19 de fevereiro de 1998**. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Diário Oficial da União, Brasília, DF, 20 fev. 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 20 out. 2024.

BRASIL. Ministério da Mulher, da Família e dos Direitos Humanos. **Lei nº 8.069, de 13 de julho de 1990.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União, Brasília, 16 jul. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 23 out. 2024.

BUFFON, Jaqueline Ana. **Agente infiltrado virtual.** In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão Criminal. Crimes cibernéticos. Brasília: MPF, 2018. (Coletânea de artigos, v. 3). Disponível em: https://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/eventos/civ-2019/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos.pdf. Acesso em: 20 jan. 2025.

CAIADO, Felipe B.; CAIADO, Marcelo. **COMBATE À PORNOGRAFIA INFANTOJUVENIL COM APERFEIÇOAMENTOS NA IDENTIFICAÇÃO DE SUSPEITOS E NA DETECÇÃO DE ARQUIVOS DE INTERESSE** In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão Criminal. Crimes cibernéticos. Brasília: MPF, 2018. (Coletânea de artigos, v. 3). Disponível em: https://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/eventos/civ-2019/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos.pdf. Acesso em: 3 set. 2025.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014.

CONTE, Christiany Pegorari; SANTOS, Coriolano Aurélio de Almeida Camargo. **Desafios do Direito Penal no mundo globalizado: a aplicação da lei penal no espaço e os crimes informáticos.** Revista de Direito de Informática e Telecomunicações, Belo Horizonte, v. 3, n. 4, p. 25–45, jan./jun. 2008.

COSTA, Marco Aurélio Rodrigues. **Crimes de informática.** Revista Eletrônica Jus Navigandi, abril 1997. Disponível em: https://jus.com.br/artigos/1826/crimes-de-informatica. Acesso em: 10 out. 2024.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** 1ª Ed. São Paulo: Saraiva, 2011. E-book.

DOMINGOS, Fernanda Teixeira Souza; RÖDER, Priscila Costa Schreiner. **Obtenção de provas digitais e jurisdição na Internet.** In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão Criminal. Crimes cibernéticos. Brasília: MPF, 2018. (Coletânea de artigos, v. 3). Disponível em: https://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/eventos/civ-2019/coletan

eas-de-artigos/coletanea_de_artigos_crimes_ciberneticos.pdf. Acesso em: 19 jan. 2025.

GRECO, Rogério. **Curso de direito penal: parte geral**. Vol. 1. 17. ed. Rio de Janeiro: Impetus, 2015.

INTERNATIONAL TELECOMMUNICATION UNION – ITU. Global Cybersecurity Index 2020. [S.l.], 2021. Disponível em: https://www.itu.int/pub/D-STR-GCI.01. Acesso em: 14 jan. 2025.

LEMOS, Ronaldo; SOUZA, Carlos Affonso. **Marco civil da internet: construção e aplicação**. Juiz de Fora Editora Associada. 2016.

MEIRELES, Isys Gonzaga; PASITTO, Fernando Teles. **ESTELIONATO E SUAS IMPLICAÇÕES: O CONSTANTE CRESCIMENTO DOS GOLPES VIRTUAIS**. Revista Ibero-Americana de Humanidades, Ciências e Educação, *[S. l.]*, v. 10, n. 11, p. 6303–6316, 2024. DOI: 10.51891/rease.v10i11.17063. Disponível em: https://periodicorease.pro.br/rease/article/view/17063. Acesso em: 6 jan. 2025.

OLIVEIRA, Neide M. C. Cardoso de; MORGADO, Marcia. **Projeto "Ministério Público pela educação digital nas escolas".** In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão Criminal. Crimes cibernéticos. Brasília: MPF, 2018. (Coletânea de artigos, v. 3). Disponível em: https://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/eventos/civ-2019/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos.pdf. Acesso em: 3 set. 2025.

RITCHIE, Hannah; MATHIEU, Edouard; ROSER, Max; ORTIZ-OSPINHA, Esteban. **Internet.** 2023. Disponível em: https://ourworldindata.org/grapher/share-of-individuals-using-the-internet. Acesso em: 4 jan. 2025.

SAFERNET Brasil. **Brasil entra no top 5 de países que mais denunciaram abuso infantil na internet em 2024.** SaferNet Brasil, 3 abr. 2025. Disponível em: https://new.safernet.org.br/content/brasil-entra-no-top-5-de-paises-que-mais-denunciaram-abuso-infantil-na-internet-em-2024. Acesso em: 4 set. 2025.

SANTOS, Humberto de Oliveira Pedra dos. **A Criminalidade Cibernética: uma análise jurídica.** Trabalho de Conclusão de Curso (Bacharelado em Direito) - Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2017. Disponível em: https://pantheon.ufrj.br/handle/11422/10826. Acesso em: 10 out. 2024.

SANTOS, Karl Heisenber Ferro. **Cibercrime: uma breve análise dos sujeitos e principais delitos virtuais.** In: ROCHA, Lilian Rose Lemos et al. (coord.). Crimes digitais. Caderno de pós-graduação em Direito. Brasília: UniCEUB: ICPD, 2020. p. 58–84. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/prefix/14602/1/Crimes%20digitais.pdf. Acesso em: 3 out. 2024.

SANTOS, L. R. dos; SOTERO, A. P. da S. **O estelionato virtual e a ineficácia da legislação brasileira para coibir o crime cibernético.** Cuadernos de Educación y Desarrollo, [S. l.], v. 16, n. 8, p. e5183, 2024. DOI: 10.55905/cuadv16n8-081. Disponível em: https://ojs.cuadernoseducacion.com/ojs/index.php/ced/article/view/5183. Acesso em: 4 jan. 2025.

SANTOS, Paulo Ernani Bergamo dos. **Direito internacional e o combate à cibercriminalidade contra crianças.** In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão Criminal. Crimes cibernéticos. Brasília: MPF, 2018. (Coletânea de artigos, v. 3). Disponível em: https://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/eventos/civ-2019/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos.pdf. Acesso em: 04 set. 2025.

SENADO NOTÍCIAS. **Golpes digitais atingem 24% da população brasileira, revela DataSenado.** Senado Notícias, 01 out. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-reveladatasenado#:~:text=Golpes%20digitais%20atingem%2024%25%20da%20popula%C3%A7%C3%A3o%20brasileira%2C%20revela%20DataSenado,-Compartilhe%20este%20conte%C3%BAdo&text=Os%20golpes%20digitais%20vitimaram%2024,brasileira%E2%80%9D%2C%20conclui%20o%20documento. Acesso em: 25 nov. 2024.

SILVA, Paulo Quintiliano da. **Dos Crimes Cibernéticos e seus efeitos internacionais.** Procedings of the Firts International Conference on Forensic Computer Science Investigation (ICoFCS´2006)/ Departamento de Polícia Federal (ed.) Brasília, Brasil, 2006. ISSN 19180-1114.

SILVA, Ângelo Roberto Ilha. Pedofilia, pornografia infantojuvenil e os tipos penais previstos no Estatuto da Criança e do Adolescente. In: SILVA, Ângelo (Org.). Crimes Cibernéticos: racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, outros temas. Porto Alegre: Livraria do Advogado, 2017.

SIQUEIRA, . N.; CONTIN, . C.; BARUFI, . B.; LEHFELD, . de S**. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD.** REVISTA ELETRÔNICA PESQUISEDUCA, [S. l.], v. 13, n. 29, p. 236–255, 2021. DOI: 10.58422/repesq.2021.e1029. Disponível em: https://periodicos.unisantos.br/pesquiseduca/article/view/1029. Acesso em: 2 out. 2024.

SOUSA, C. M. R. de; SANTOS, G. A. M. **Crimes cibernéticos e os desafios jurídicos na era digital: análise legislativa, doutrinária e jurisprudencial.** Revista JRG de Estudos Acadêmicos, Brasil, São Paulo, v. 7, n. 15, p. e151662, 2024. Disponível em: https://revistajrg.com/index.php/jrg/article/view/1662. Acesso em: 8 jan. 2025.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. **Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da**

Internet. 2017; UNIVERSIDADE DE FORTALEZA; Volume: 22; Issue: 1 Linguagem: Português. Disponível em: https://ojs.unifor.br/rpen/article/view/6272/pdf. Acesso em: 4 set. 2025.

VALLE, Sabrina. **Carolina Dieckmann teve as fotos roubadas por hackers.** O Estado de S. Paulo, São Paulo, 14 maio 2012, p. C7.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: ameaças e procedimentos de investigação.** 2 ed. Rio de Janeiro: Brasport, 2013.

WORLD HEALTH ORGANIZATION – WHO. **The ICD-10 Classification of Mental and Behavioural Disorders – Diagnostic criteria for research.** 1993. Disponível em: https://www.who.int/classifications/classification-of-diseases. Acesso em: 3 set. 2025.

ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro: parte geral.** 11. ed. São Paulo: Revista dos Tribunais, 2015.