Revista Jurídica do Nordeste Mineiro, v.5, 2024
ISSN 2675-4312

O TRATAMENTO JURÍDICO DOS CRIMES VIRTUAIS COM BASE NA LEGISLAÇÃO BRASILEIRA

THE LEGAL TREATMENT OF VIRTUAL CRIMES BASED ON BRAZILIAN LEGISLATION

Leandro Sousa Ruas

Aluno do 9º período do curso de Direito da Faculdade AlfaUnipac-

Teófilo Otoni/MG, Brasil.
E-mail: lruas8000@gmail.com

Lorenzo Jardim Pinas

Aluno do 9º período do curso de Direito da Faculdade AlfaUnipac-

Teófilo Otoni/MG, Brasil.
E-mail: lorenpvp@gmail.com

Saulo Emanuel Araújo de Sousa

Aluno do 9º período do curso de Direito da Faculdade AlfaUnipac-

Teófilo Otoni/MG, Brasil.
E-mail: sa6718091@gmail.com

Erica Oliveira Santos Gonçalves

Bacharel em direito, especialista em direito processual, advogada, professora de Direito Penal e Processo Penal da Universidade Presidente Antonio Carlos - Faculdade de Direito de Teófilo Otoni/MG -UNIPAC, E-mail: erica.almenara@gmail.co

Resumo

O presente artigo aborda o tratamento jurídico dos crimes virtuais no contexto da legislação brasileira. Inicialmente, foi definido o conceito da internet e sua evolução para o ambiente digital global presente na atualidade. Em seguida, foi traçado um breve histórico dos crimes cibernéticos, destacando seu crescimento exponencial e os principais desafios enfrentados. Também foram abordados os principais setores impactados por esses crimes, incluindo empresas, instituições governamentais e

indivíduos, e discutidos os principais delitos cometidos, como estelionato, extorsão, crimes contra a honra, pornografia infantil e invasão de dispositivos informáticos; bem como as táticas utilizadas pelos criminosos cibernéticos para cometer esses crimes, destacando sua sofisticação e adaptabilidade. E, por fim, foi analisado como a legislação brasileira atua no combate aos crimes virtuais, com destaque para o Marco Civil da Internet, a Constituição Federal, a Lei Geral de Proteção de Dados (LGPD) e a Lei Carolina Dieckmann. Essas leis estabelecem diretrizes para proteger os direitos dos cidadãos no ambiente digital, garantindo a liberdade de expressão, a privacidade e a segurança das informações pessoais.

Palavras-chave: Internet; Crimes cibernéticos; Privacidade.

Abstract

The article addresses the legal treatment of virtual crimes in the context of Brazilian legislation. Initially, the concept of the internet and its evolution into the global digital environment present today was defined. Next, a brief history of cybercrimes was outlined, highlighting its exponential growth and the main challenges faced. The main sectors impacted by these crimes were also addressed, including companies, government institutions and individuals, and the main crimes committed were discussed, such as embezzlement, extortion, crimes against honor, child pornography and invasion of computer devices; as well as the tactics used by cybercriminals to commit these crimes, highlighting their sophistication and adaptability. And, finally, it was analyzed how Brazilian legislation acts to combat virtual crimes, with emphasis on the Marco Civil da Internet, the Federal Constitution, the General Data Protection Law (LGPD) and the Carolina Dieckmann Law. These laws establish guidelines to protect the rights of citizens in the digital environment, guaranteeing freedom of expression, privacy and security of personal information.

Keywords: Internet; Cyber crimes; Privacy.

1. Introdução

Na era digital, a internet se tornou um espaço vital para a interação humana, o compartilhamento de informações e o desenvolvimento de atividades comerciais e governamentais. No entanto, junto com os benefícios proporcionados pela conectividade global, surgiram também os desafios relacionados aos crimes virtuais, que afetam indivíduos, empresas e instituições em todo o mundo.

Neste contexto, é essencial compreender o tratamento jurídico dos crimes cibernéticos sob a perspectiva da legislação brasileira. Desde os primórdios da internet, crimes como estelionato, extorsão, crimes contra a honra, pornografia infantil e invasão de dispositivos informáticos têm sido cometidos, causando danos significativos às vítimas e à sociedade como um todo.

Dentre os setores impactados por esses crimes, destacam-se empresas, que sofrem com fraudes financeiras e roubo de informações sensíveis, e indivíduos, que têm sua privacidade violada e sofrem ataques à sua honra e reputação. Os criminosos cibernéticos operam de maneira astuta, aproveitando-se das vulnerabilidades dos sistemas de segurança e da ingenuidade das vítimas.

No entanto, a legislação brasileira tem buscado enfrentar esse desafio, por meio de instrumentos como o Marco Civil da Internet, a Constituição Federal, a Lei Geral de Proteção de Dados (LGPD) e a Lei Carolina Dieckmann. Essas leis estabelecem diretrizes para proteger os direitos dos cidadãos no ambiente digital, garantindo a liberdade de expressão, a privacidade e a segurança das informações pessoais.

Neste artigo, será explorado com mais detalhadamente o conceito da internet, o histórico dos crimes cibernéticos, os setores impactados por esses crimes, os principais delitos cometidos e como os criminosos cibernéticos agem. Além disso, será analisado como a legislação brasileira atua no combate aos crimes virtuais, com destaque para o Marco Civil, a Constituição Federal, a LGPD e a Lei Carolina Dieckmann. Ao compreender melhor esse cenário, será possível enfrentar os desafios e construir um ambiente digital mais seguro e confiável para todos.

2 Internet: conceito e desenvolvimento

Na década de 60, ainda durante a Guerra Fria, a fim de criar uma estratégia para proteger informações valiosas de potenciais ataques, o Departamento de Defesa dos Estados Unidos desenvolveu uma rede descentralizada de comunicação. Essa rede recebeu o nome de ARPANET, em alusão a ARPA, uma das subdivisões do departamento de defesa americano (CONTENT, R., 2020).

A ARPANET, como ficou conhecida, era uma rede subterrânea ligada por um backbone, o que possibilitava a troca de informações sigilosas entre as bases estratégicas americanas, bem como traçar planos de combate e identificar casos de ameaças de outros países. Inicialmente, seu acesso era restrito aos militares e pesquisadores, apenas nos anos seguintes a ARPAnet serviu de inspiração para a criação de uma rede global que permitisse a comunicação simultânea de computadores de qualquer lugar do mundo (HOSTINGER, 2023).

Apenas no início dos anos 70 surgiu o termo “internet”, no qual se referia a interconexão de redes através de protocolos TCP e IP (Transmission Control Protocol / Internet Protocol), baseados em serviços de internet e e-mails. Após o seu lançamento e até os dias atuais a internet sofreu diversos processos de evolução, o que permitiu o desenvolvimento de programas, plataformas e outros serviços (PAREDES, A., 2019).

Como mencionado, a internet passou por radicais processos de transformação desde a sua criação, o que era usado como um espaço de armazenamento de informações e trocas de e-mails deu lugar ao desenvolvimento da “internet das coisas”, estando presente em objetos e lugares por todo o mundo (CONTENT, R., 2020).

No que pese a tecnologia representar um marco de evolução profundo em nossa sociedade, a forma como ela é utilizada pode ensejar benefícios ou desafios para o usuário. Diante do avanço tecnológico acelerado, é necessário que se reflita sobre seus impactos na vida das pessoas. Atualmente, esse avanço tecnológico possibilitou o avanço em diversas áreas profissionais e sociais, como na medicina, no mercado de trabalho. Por outro lado, possibilitou, também, que pessoas de diversos países pudessem se comunicar uma com as outras de onde quer que estejam, o que não deixa de ser um ponto positivo, porém, essa conexão de redes tem resultado em uma grande exposição de ataques cibernéticos, como golpes, sequestro de dados, e outros crimes que serão destacados ao logo desse artigo (TECNOLOGIA, P., 2019).

3 Crimes Cibernéticos

Com o crescente avanço da tecnologia, a internet tem ganhado mais espaço na vida das pessoas em praticamente todos os cantos do planeta. A internet trouxe muitos benefícios para a humanidade como, por exemplo, o acesso à informação de modo instantâneo e com diversos modelos de mídias, como notícias jornalísticas, reportagens, documentários, filmes etc. A praticidade é outro exemplo disso, pois através dela é possível fazer compras sem sair de casa, realizar reuniões, estudar, trabalhar. Sem contar outras possibilidades, como entretenimento, relacionamento e outros (TELECOM, 2021).

Entretanto, nem tudo é maravilha no mundo digital, já que em decorrência do

incessante avanço da tecnologia surgem diversos desafios a serem superado, como os crimes cibernéticos, considerados como uma realidade inegável no ambiente digital.

3.1 Breve histórico dos crimes cibernéticos e conceituação

O primeiro delito informático registrado na humanidade ainda é alvo de divergência na doutrina. Conforme alguns, foi em 1964 quando ocorreu a primeira ação considerada *cibercrime*, ocorrida dentro do Instituto de Tecnologia de Massachusetts. Já para outros, o primeiro caso ocorreu em 1978, quando se mencionou pela primeira vez o termo *hacker.* No entanto, apenas nas décadas de 80 e 90 que houve a propagação de vários casos de *cibercrime*,sendo as condutas de disseminação de vírus, pornografia infantil, pirataria e invasão de sistemas as mais comuns (JESUS, Damasio, 2016).

Os crimes virtuais, ou cibernéticos, abrangem uma série de atividades ilícitas, que ocorrem, principalmente, em decorrência do uso inadequado de computadores, dispositivos eletrônicos e dos ambientes virtuais em geral. Destaca-se que esses não se limitam apenas ao espaço virtual, já que é possível a ocorrência de crimes mesmo em ambiente offline, ou seja, ainda que o dispositivo não esteja efetivamente conectado à internet. As atividades criminosas vão desde a ataques brutais de malware, até sofisticadas fraudes envolvendo criptomoedas, e abordagens diversas com ferramentas cada vez mais avançadas (NEON, 2023).

3.2 Principais setores impactados

Os principais setores impactados por esses criminosos possuem ligação diretamente com ativos financeiros. Porém, também se destacam os crimes ligados à violação de privacidade, incluindo aquelas de natureza sexual, vazamento de informações sensíveis, cyberbullying e as famosas “fake News”, ou simplesmente a disseminação de notícias falsas. Não se pode deixar de mencionar, também, os incidentes envolvendo *ransomware* na área da saúde, pois conforme a Check Point Reserach (CPR), apenas no segundo semestre de 2022, esse setor sofreu um aumento de 5% nos ataques (HOSTDIME, 2023).

No entanto, esses ataques não se limitam a apenas esse setor, pois as

ameaças cibernéticas também estão presentes nos setores de tecnologia, o que requer maior investimento em segurança da informação. Outra área que tem apresentado vulnerabilidade diante desses ataques é a de energia, pois conforme a Agência Nacional de Energia Elétrica (Aneel), inviabilização de operações técnicas, perda de dados das empresas e interrupções no suprimento de energia são apenas alguns dos desafios a serem superados. Já outro dado que requer atenção é com relação aos apresentados em razão de ameaças ao setor governamental, pois apenas no segundo semestre de 2022 houve um aumento de 95% em ataques governamentais em todo o mundo, sendo que os principais estão relacionados a ataques de negação de serviço (DDos), conforme relatório da CloudSek (CLARANET, 2023).

3.3 Principais tipos de crimes cibernéticos

Conforme mencionado, os crimes cibernéticos são tipos de ataques criminosos ocorridos em ambiente virtual, em que as principais ferramentas utilizadas para isso são os computadores ou dispositivos móveis, rede de computadores ou outros dispositivos conectados a essa rede. Grande parte desses ataques ocorrem visando ganhos financeiros. Contudo, não se descarta a possibilidade de ataques visando apenas interesses pessoais ou políticos, sendo que esses, geralmente, visam apenas a danificação de dispositivos ou redes (KASPERSKY, 2024).

Só no ano de 2022, conforme levantamento da Fortinet, o Brasil sofreu mais de 100 bilhões de tentativas e ameaças de ataques cibernéticos, o que representa cerca de 30% dos ataques registrados em toda a américa. Ressalta-se que o principal crime cometido é o de *phishing,* que se refere a uma técnica criminosa usada para obter dados e informações confidenciais de maneira fraudulenta (JORNAL DA USP, 2023).

Os crimes virtuais são praticados por indivíduos ou grupos organizados que almejam, em grande parte, obter vantagens financeiras, informações pessoais, ou simplesmente provocar a interrupção de serviços ou a perda de dados ou informações sensíveis. Esses crimes podem ser caracterizados de diversas formas, mas neste artigo será dado ênfase aos crimes contra o patrimônio em geral, fraudes eletrônicas e contra as pessoas (BUGHUNT, 2023).

No que pese o cometimento de crimes pela internet, pode-se utilizar legislações já existentes no ordenamento jurídico brasileiro para regular essas práticas ilegais, como é o caso do Código Penal, quanto aos crimes de calúnia, pornografia, estelionato etc. Assim, o que é levado em consideração são as condutas praticadas, sejam ação ou omissão, e não a maneira como se deu a conduta. Conforme Tarcísio Teixeira explica:

> Às vezes, a maneira pela qual se pratica o crime pode ser uma qualificadora que aumenta a pena, assim como quando se usa fogo ou veneno para a prática do homicídio. São, então, os denominados crimes de informática impróprios (crimes já existentes, mas que são praticados usando o ferramental da informática), dentre os quais discorreremos sobre os que consideramos de maior relevância. Devemos alertar o leitor que, do exame que se segue, algumas tipificações penais sofreram ajustes em suas redações originais, a fim de prever determinadas condutas praticadas com o uso da informática ou contra sistema de informática (alguns podendo ser tidos como crimes de informática próprios), minimizando possíveis atipicidades criminais para certas ações humanas (TEIXEIRA, 2022, p.448/449).

Dessa forma, pode-se dizer que os crimes informáticos podem ser caracterizados como crimes impróprios quando a tecnologia da informação ou a internet é utilizada como um meio para ofender bens jurídicos já tipificados como crimes pelo Código Penal. Já os crimes informáticos próprios decorrem diretamente da ofensa contra a tecnologia da informação (TEIXEIRA, 2023).

3.3.1 Crimes contra o patrimônio

Grande parte dos crimes praticados em meios tecnológicos são relacionados aos crimes contra o patrimônio, como o estelionato, extorsão, dano etc. Esses crimes podem ter como vítimas tanto pessoas físicas quanto jurídicas. Como mencionado anteriormente, esses crimes mantem a mesma conduta mencionada nos crimes tipificados no código penal, com a única peculiaridade de que é praticado em meio virtual (TEIXEIRA, 2022).

O crime de estelionato praticado em ambiente eletrônico pode ser facilmente identificado quando criminosos usam de artifícios fraudulentos para induzir ou manter algum usuário da internet a erro, a fim de obterem vantagem ilícita, como ocorre quando um indivíduo clona sites ou envia um e-mail se passando por alguma instituição ou outra pessoa, como os principais objetivos de obter dados bancários ou informações pessoais, e com isso conseguir realizar transferências bancárias.

Outro crime contra o patrimônio que, também, pode ocorrer por meios virtuais é o de extorsão e, assim como tipificado no art. 158 do Código Penal, este crime ocorre quando há a existência de constrangimento e violência ou grave ameaça, a fim de obter vantagem econômica. A sua prática pode ser identificada quando os criminosos retiram algum site do ar e logo após pede uma espécie de "resgate" para voltar o seu funcionamento normal (BARBOSA, 2019).

Crimes contra fraudes em geral também ocorre com frequência nos meios virtuais. Grande parte desses golpes ocorrem através de leiloes, pirâmides, promessas de altos ganhos, ou até mesmo através de spam, utilizados para propagar vírus ou anunciar publicidades enganosas ou abusivas (TEIXEIRA, 2022).

3.3.2 Crimes contra a honra

Outras condutas tipificadas no Código Penal que podem ocorrer em ambiente virtual são os crimes contra a honra, como a calúnia, a difamação e a injúria. O CP ensina que o crime de calúnia ocorre quando, falsamente, é imputado a alguém um fato caracterizado como crime, conforme artigo 138. Um exemplo disso é quando alguém, sem provas, posta nas redes sociais o nome e a foto de outra como autor de um homicídio. Já a difamação (art. 139 do CP), refere-se à imputação de um fato ofensivo à reputação de alguém, como a exposição de detalhes da vida pessoal de outra pessoa, ainda que haja provas dos fatos alegados. Por outro lado, a injúria (art.140 do CP), trata-se de ofensa à dignidade ou decoro, ocorre, por exemplo, quando um indivíduo faz comentários em perfis da internet com o objetivo de ofender atributos físicos ou intelectos daquela pessoa, como "baleia", "quatro olhos" etc (EL DEBS, 2022).

Vale ressaltar sobre a possibilidade de aplicabilidade de uma agravante nos crimes contra a honra praticados na internet. Conforme o §2º do art. 142, do Código Penal, a pena para esses crimes, nessa modalidade, pode ser triplicada: *§ 2º Se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena* (BRASIL, 1940).

Destaca-se que o termo "redes sociais" refere-se a vários aplicativos espalhados pela internet como, por exemplo, Whatsapp, Instagram, Telegram, Facebook e outros. Assim, é possível que a pena para esses crimes seja triplicada ainda que as conversas tenham ocorrido em chats ou grupos privados (EL DEBS,

2022).

3.3.3 Pornografia Infantil e Pedofilia

Inicialmente, é importante que não se confunda o crime de pornografia infantil com pedofilia. Pois aquele está previsto na Lei de nº 8.069/90, também conhecia como Estatuto da Criança e do Adolescente (ECA); Por outro lado, a pedofilia é considerada como uma anomalia, em que o indivíduo sente atração por crianças, nestes casos não há punibilidade para esse indivíduo, já que a legislação brasileira não apresenta uma punição específica para pedofilia física e virtual. No entanto, há projetos de lei em andamento com o objetivo de incluir esses tipos de crimes no código penal (NAZAR, 2023).

É importante destacar que o artigo 241-A foi incluído no Estatuto da Criança e do Adolescente através da Lei n 11.829/2008, passando dispor o seguinte:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de **sistema de informática ou telemático**, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1 º Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso **por rede de computadores** às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2 º As condutas tipificadas nos incisos I e II do § 1 º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo (grifos nossos).

O Projeto de Lei (PL 830/2022), do Senador Flávio Bolsonaro (PL-RJ), prever o aumento da pena de 5 para 8 anos de prisão, além da multa para quem registrar, vender e expor pornografia infantil. Ademais, o texto da PL também prever a internet como possível meio de aliciamento, instigação e assédio de crianças. Ressalta-se que as penas para esses crimes já existem, o projeto requer o aumento para essas penas (SENADO, 2023).

É necessário que os pais ou responsáveis fiquem alertas com o uso de internet e, principalmente, redes sociais e jogos por crianças ou adolescentes, pois com o avanço da tecnologia, especialmente, da Inteligência Artificial, criminosos tem usado desses artifícios para conseguirem atrair a atenção de crianças sem que levante suspeitas, como ocorre através do “deepfake”, capaz de alterar voz, rosto e

corpo dos criminosos (ARAÚJO, 2023).

3.3.4 Invasão de dispositivo informático

A Lei n. 12.737/2012 adicionou ao Código Penal o art. 154-A, que criminaliza a invasão de dispositivo informático. Esse crime consiste em acessar indevidamente um dispositivo alheio, com ou sem conexão à internet, violando suas medidas de segurança, com a intenção de obter, adulterar ou destruir dados sem autorização do titular (TEIXEIRA, 2022).

O elemento subjetivo é o dolo, e o crime pode ser cometido mesmo offline. Não é crime invadir dispositivos próprios ou de terceiros com consentimento, sendo assim, a invasão deve ser em relação à invasão de dispositivo alheio e de forma indevida. Outro ponto a ser observado é que o dispositivo invadido deve conter algum mecanismo de segurança, como antivírus, *firewall,* senhas etc., pois caso contrário a conduta torna-se atípica (PEREIRA, 2023).

Aqueles que distribuem programas para facilitar essa prática também são responsabilizados. Em casos de controle remoto não autorizado ou obtenção de informações privadas, a pena é de reclusão, e aumenta se houver divulgação ou comercialização dos dados obtidos (BARBOSA, 2020).

3.4 Breve análise do perfil dos criminosos e formas de ataques

O termo "criminoso" refere-se ao agente ativo do crime de informática. Embora qualquer pessoa possa ser um infrator nesse campo, muitos desses crimes são cometidos por indivíduos com profundos conhecimentos em Tecnologia da Informação. Muitas vezes, a internet serve como prova para identificar o criminoso em casos como compartilhamento de imagens de cadáveres, que pode configurar o crime de vilipêndio a cadáver. Os criminosos da internet, conhecidos como piratas cibernéticos, geralmente são jovens, do sexo masculino, educados, audaciosos e com alta inteligência, que utilizam seu conhecimento técnico e habilidades intelectuais para cometer crimes, muitas vezes sem contato direto com a vítima (TEIXEIRA, 2022).

O anonimato proporcionado pela internet é um facilitador significativo para os criminosos, permitindo que cometam delitos sem identificação precisa ou presença

física no local do crime. Isso inclui a utilização de perfis falsos em redes sociais e a engenharia social para explorar a falta de informação das vítimas. No Brasil, a falta de legislação específica e de especialização jurídica, tanto por parte dos legisladores quanto dos magistrados, contribui para a prevalência desse tipo de crime. Além disso, há uma escassez de delegacias especializadas em crimes cibernéticos, o que torna a investigação e punição desses delitos ainda mais desafiadoras (TELECO, 2024).

Os métodos mais comuns de ataques cibernéticos são conhecidos como *Malware, Ransomware*, Roubo de identidade, e outros fraudes já citadas anteriormente. Os *malwares* São códigos maliciosos instalados em dispositivos sem o conhecimento do usuário, frequentemente disfarçados como downloads falsos ou sites clonados. Podem ser usados para espionagem empresarial, roubo de credenciais ou modificação de dados sem detecção. Já o *ransomware* destaca-se por sua nocividade, criptografando dados da empresa e exigindo um resgate em dinheiro para restaurar o acesso. Já no roubo de identidade, os criminosos acessam dados pessoais e credenciais para se passarem por outras pessoas, realizando fraudes financeiras e comerciais ou comprometendo informações sensíveis de empresas (CLEARSALE, 2022).

4 Legislação brasileira no tratamento dos crimes virtuais: Principais legislações

O Brasil está consideravelmente atrasado em termos de legislação penal relacionada à informática. A revolução tecnológica apresenta desafios significativos ao Direito Penal, com muitos casos que requerem adaptação às leis existentes. Existem diversos Projetos de Lei no Congresso que tentaram abordar condutas cometidas no ambiente cibernético, porém muitos deles são propostas inadequadas por falta de compreensão do problema. Os crimes informáticos se beneficiam do anonimato e da baixa probabilidade de punição, devido à falta de legislação específica. Até recentemente, o Brasil possuía poucas leis relacionadas a crimes informáticos, com a Lei n. 9.983/2000 sendo a principal referência, mas aplicável principalmente a funcionários públicos (JESUS, 2016).

4.1 Constituição Federal e Internet

A Constituição Federal Brasileira é o principal documento jurídico do país e serve como base para todo o ordenamento legal, incluindo a abordagem de crimes cibernéticos. Embora não haja disposições específicas sobre crimes cibernéticos na Constituição, diversos princípios e garantias constitucionais são aplicáveis a esse contexto.

4.1.1 Privacidade e intimidade

Pode-se dizer que a privacidade se refere ao conjunto de informações sobre um indivíduo que ele pode optar por manter sob seu controle exclusivo ou compartilhar com outros de acordo com suas condições desejadas. É associada ao que é privado e de conhecimento restrito, ao contrário do que é público e de conhecimento geral. Segundo Tércio Sampaio Ferraz Júnior, a privacidade diz respeito apenas ao indivíduo, incluindo sua vida familiar e íntima, que devem ser guardadas por ele de maneira discricionária (TEIXEIRA, 2022).

O artigo 5, inciso X, dispõe que: *"são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"*. É importante destacar que a intimidade não se confunde com privacidade, já que a vida privada consiste em informações que apenas a pessoa pode decidir se divulga ou não. Por outro lado, a intimidade refere-se ao modo de ser da pessoa, sua identidade, que pode ser confundida com a vida privada (BOAZ, 2015).

Considerando a violação da privacidade e da intimidade nos ambientes virtuais, é importante destacar, que praticamente todos os nossos dados estão registrados de alguma forma, incluindo informações acessíveis em nossos celulares, como dados pessoais armazenados pelo Google e Facebook, bem como informações bancárias. As conversas no WhatsApp podem ser utilizadas para traçar um perfil detalhado de nossas vidas e relacionamentos. O conteúdo de um computador pessoal também pode revelar aspectos íntimos de nossa vida. A falta de proteção desses dados representa um risco à efetivação dos direitos à intimidade e privacidade, exigindo uma abordagem mais rígida em relação ao acesso e manipulação dessas informações (GARCIA, 2017).

4.1.2 Liberdade de expressão

Nenhum país democrático considera a liberdade de expressão um direito ilimitado. As disputas em torno desse direito não se limitam apenas às leis, mas também envolvem áreas como religião, jornalismo, universidades e internet. Esses embates têm evoluído ao longo dos anos. No século 20, a liberdade de expressão foi reconhecida como um direito universal. Em 1948, a Assembleia-Geral das Nações Unidas (ONU) incluiu o conceito na Declaração Universal dos Direitos Humanos, estabelecendo que "todo ser humano tem direito à liberdade de opinião e expressão", incluindo a busca, recebimento e transmissão de informações por quaisquer meios, sem interferência e independentemente de fronteiras. Nos países democráticos atuais, os limites à liberdade de expressão são definidos por leis que punem crimes relacionados à expressão, como incitação à violência, sedição, difamação, calúnia, blasfêmia, racismo e conspiração (MAGENTA, 2022).

De acordo com a teoria constitucional brasileira, a liberdade de expressão abrange uma ampla gama de manifestações individuais e coletivas, como a liberdade de pensamento, opinião, imprensa, acadêmica e de crítica. Seu objetivo principal é garantir um ambiente democrático onde as pessoas possam se expressar sem interferência do Estado ou de outras entidades, contribuindo para o debate público, o pluralismo de ideias e o desenvolvimento da sociedade. Apesar de garantir a liberdade de expressão, o inciso IV do art. 5º da Constituição estabelece uma vedação ao anonimato, visando também proteger o direito de resposta e a indenização por danos materiais, morais ou à imagem (MARTINELLI, 2023).

O art. 220 da CF também destaca acerca da liberdade de expressão vedando qualquer forma de censura política, ideológica e artística aos meios de comunicação social. Ele também estabelece que as diversões e espetáculos públicos são livres, desde que observem recomendações quanto à faixa etária, local e horário. Além disso, a propaganda comercial de produtos prejudiciais à saúde e ao meio ambiente, como tabaco, bebidas alcoólicas, agrotóxicos, medicamentos e terapias, está sujeita a restrições mais rígidas, assim como a comunicação dirigida a crianças (MENDES, 2023).

Já a liberdade de expressão na internet refere-se ao direito das pessoas de expressarem livremente suas opiniões, ideias e pensamentos através das redes. No entanto, esse direito enfrenta desafios devido à desigualdade de acesso à internet e

à censura governamental em alguns países, como na China, onde existe o Grande Firewall que limita o acesso a sites estrangeiros e restringe a liberdade de expressão online. Além disso, a vigilância em massa realizada por governos, como revelado por Edward Snowden em 2013, gerou debate sobre privacidade e segurança dos dados dos usuários. O principal desafio é encontrar um equilíbrio entre a liberdade de expressão e outros direitos fundamentais, como a dignidade, segurança e privacidade, para promover um ambiente digital inclusivo e democrático (MENDES, 2023).

4.2 Marco civil da internet

A Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet (MCI), tem sido apelidada por alguns como a "Constituição da Internet". Essa legislação estabelece uma posição clara do Brasil em relação à proteção jurídica da liberdade de expressão e da privacidade na internet. Tal lei pode ser considerada como uma legislação principiológica, já que estabelece parâmetros gerais sobre princípios, garantias, direitos e deveres para o uso da internet no Brasil. Além disso, ela determina diretrizes a serem seguidas pelo Poder Público. O texto da lei também inclui regras específicas para agentes que operam na internet, especialmente para provedores de conexão e de aplicações de internet (TEIXEIRA, 2022).

O Marco Civil da Internet trouxe uma inovação significativa em seu processo legislativo, que incluiu um debate aberto com participação direta da sociedade. Durante aproximadamente 7 anos, de 2007 a 2014, a elaboração e desenvolvimento da legislação foram realizados por meio de consultas públicas, utilizando a internet para colher opiniões de diversos grupos sociais. Esse processo assemelhou-se a um "fórum de discussão na internet", onde as pessoas detalhavam os princípios e podiam propor novos temas a serem abordados pela legislação (RAMOS, 2021).

Na época, houve um debate polarizado em relação à intervenção do Estado no ambiente digital. Enquanto alguns defendiam a não interferência estatal, argumentando que isso permitiria inovação contínua e destacando que "O código de programação é a própria lei", outros acreditavam que o governo deveria editar normas para regular os comportamentos online, a fim de evitar arbitrariedades por parte dos que controlam a internet devido à inércia estatal (RAMOS, 2021).

Portanto, o Marco Civil representa um grande avanço para o direito digital no Brasil, ao estabelecer direitos aos usuários da internet, como inviolabilidade da intimidade e vida privada, manutenção da qualidade da conexão contratada, aplicação de normas do direito do consumidor entre outros, bem como ao estabelecer deveres aos provedores de internet e de aplicações. Ademais, a lei tem como objetivo proteger a privacidade, a liberdade de expressão e a neutralidade da rede, além de regular responsabilidades de provedores de internet e garantir a segurança dos usuários. O Marco Civil é considerado uma referência internacional em termos de legislação para a internet e teve um papel importante na definição de diretrizes para o uso da rede no Brasil (FACHINI, 2022).

4.3 Lei Geral de Proteção de Dados Pessoais- LGPD (LEI N. 13.709/2018).

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, tem como objetivo proteger os direitos fundamentais de liberdade e privacidade, bem como a formação da personalidade de cada indivíduo. Ela aborda o tratamento de dados pessoais, realizados por pessoas físicas ou jurídicas, tanto de direito público quanto privado, em meios físicos ou digitais. A lei define dois agentes de tratamento de dados - o Controlador e o Operador - e estabelece a figura do Encarregado, responsável pela comunicação entre os agentes de tratamento, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O tratamento de dados abrange uma ampla gama de atividades, como coleta, processamento, armazenamento, transmissão e eliminação de informações pessoais (BRASIL, 2021).

Ademais, a LGPD estabelece diretrizes para o tratamento de dados pessoais no Brasil, afetando tanto indivíduos quanto empresas e entidades governamentais. Desde sua entrada em vigor em agosto de 2020, a lei tem impacto significativo na administração pública, abrangendo órgãos dos poderes Executivo, Legislativo e Judiciário, bem como autarquias e fundações. O setor público precisa se adequar aos princípios da LGPD, como finalidade, transparência e segurança dos dados. Para isso, é necessário investir em tecnologia, processos e capacitação de pessoal (BRASIL, 2023).

Essa Lei impõe obrigações às empresas sobre a coleta, armazenamento, tratamento e compartilhamento de dados, tanto online quanto offline. Uma

característica importante é sua aplicação extraterritorial, o que significa que a lei se aplica independentemente da localização da empresa, desde que os dados pertençam a cidadãos brasileiros ou tenham sido coletados no Brasil. O GDPR, regulamentação europeia sobre proteção de dados, foi uma influência importante na criação da LGPD e serviu de modelo para muitos outros países adotarem medidas semelhantes (NONES, 2022).

Conforme o art. 52 da referida lei, a LGPD prevê sanções administrativas que podem ser aplicadas em caso de descumprimento: *Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional*.

Essas sanções têm o objetivo de garantir o cumprimento da legislação e proteger os direitos dos titulares dos dados, variando desde advertências, multa simples, multa diária, bloqueio de dados pessoais, suspensão parcial do funcionamento de banco de dados e outras penalidades.

4.4 Lei nº 12.737/2012: Lei Carolina Dieckman

Em 2022 comemorou-se 10 anos de vigência da Lei Carolina Dieckman. A referida lei é considerada a primeira a punir crimes cibernéticos no país. A Lei ganhou relevância a partir do caso da atriz Carolina Dieckmann em 2011, quando teve seu computador pessoal invadido e fotos íntimas divulgadas após não ceder à extorsão dos criminosos. Antes da lei, invadir ambientes virtuais e subtrair dados pessoais já era crime, mas não havia legislação específica sobre o assunto. Em 2012, foi proposto um projeto de lei para abordar invasões de dispositivos eletrônicos e o uso indevido de informações obtidas. O projeto visava criminalizar o uso indevido de informações pessoais na internet, como fotos e vídeos, e combater fraudes financeiras eletrônicas (ARAÚJO, 2023).

Importante destacar que antes da Lei nº 12.737/2012, acessar dispositivos informáticos para obter ou destruir dados era considerado apenas atos preparatórios e não puníveis. Isso significava que, se não houvesse exigência de vantagem econômica ou prejuízo causado, o agente não era responsabilizado criminalmente. Em 2021, a legislação foi modificada para permitir a punição mesmo quando o dispositivo não está protegido por senha e quando o prejudicado não é o

proprietário. Isso significa que se alguém tiver dados capturados sem autorização em um dispositivo, mesmo que não seja o proprietário, o ato constitui crime. Além disso, as penas foram aumentadas para reclusão, permitindo a interceptação das comunicações telemáticas (REINA, 2022).

5 Conclusão

Diante do cenário cada vez mais presente da sociedade digital, a questão do tratamento jurídico dos crimes virtuais assume uma importância fundamental. A internet, concebida como um espaço livre e democrático de troca de informações e interação, tem sido palco para uma série de crimes cibernéticos, que vão desde o estelionato até a pornografia infantil e a invasão de dispositivos informáticos.

Esses crimes têm impactado diversos setores da sociedade, incluindo empresas, instituições governamentais e indivíduos, causando prejuízos financeiros, danos à reputação e violações à privacidade. Os criminosos cibernéticos agem de maneira sofisticada, aproveitando-se de falhas na segurança digital e explorando a ingenuidade e vulnerabilidade das vítimas.

A legislação brasileira tem buscado se adequar a esse novo contexto, com instrumentos como o Marco Civil da Internet, a Constituição Federal, a Lei Geral de Proteção de Dados (LGPD) e, de maneira emblemática, a Lei Carolina Dieckmann. Essas leis estabelecem diretrizes para proteger os direitos dos cidadãos no ambiente digital, garantindo a liberdade de expressão, a privacidade e a segurança das informações pessoais.

No entanto, apesar dos avanços legislativos, ainda há desafios a serem enfrentados. A efetividade da aplicação da lei e a capacidade de investigação e punição dos criminosos cibernéticos nem sempre são garantidas. Além disso, a constante evolução da tecnologia requer uma atualização constante das normas jurídicas para acompanhar as novas formas de crime digital.

Diante desse contexto, é fundamental um esforço conjunto entre governo, setor privado, sociedade civil e órgãos de segurança para combater os crimes virtuais e proteger os direitos dos cidadãos no ambiente digital. Somente com uma abordagem integrada e multidisciplinar será possível construir um ambiente virtual mais seguro e confiável para todos.

Referências

AGÊNCIA SENADO. **Pornografia infantil poderá ter pena aumentada para 8 anos de cadeia.** 2023. Disponível em: <https://www12.senado.leg.br/noticias/materias/2023/12/06/pornografia-infantil-podera-ter- pena-aumentada-para-8-anos-de-cadeia>. Acesso em 20 de março de 2024.

ARAÚJO, Aurélio. Não é só na novela: pedófilos utilizam táticas online para aliciar menores. 2023. Tilt Uol. Disponível em:<https://www.uol.com.br/tilt/noticias/redacao/2023/03/29/pedofilos-aliciamento-menores- online.htm >. Acesso em: 14 de março de 2024.

BARBOSA, Adriano. **Do crime de invasão de dispositivo informático**. Gran, 2020. Disponível em: <https://blog.grancursosonline.com.br/do-crime-de-invasao-de-dispositivo- informatico/ >. Acesso em: 21 de fevereiro de 2024.BARBOSA, Carina Luna**. Crimes cibernéticos: Crimes de alta tecnologia.** 2019. Disponível em: <https://www.jusbrasil.com.br/artigos/crimes-ciberneticos-crimes-de-alta-tecnologia/686479261 >. Acesso em 20 de março de 2024.

BLOG ROCK CONTENT. **Conheça a história da internet, sua finalidade e qual o cenário atua**l. 2020. Disponível em: <https://rockcontent.com/br/blog/historia-da-internet/ >. Acesso em 10 de março de 2024.

BOAZ, Raul**. Intimidade e privacidade sob a ótica do Direito Brasileiro**. Jus.com, 2015. Disponível em: <https://jus.com.br/artigos/38335/intimidade-e-privacidade-sob-a-otica-do- direito-brasileiro >. Acesso em 06 de março de 2024.

BRASIL, 2023. **Pornografia infantil poderá ter pena aumentada para 8 anos de cadeia**. Senado Notícias, 2023. Disponível em: < https://www12.senado.leg.br/noticias/materias/2023/12/06/pornografia-infantil-podera-ter- pena-aumentada-para-8-anos-de-cadeia>. Acesso em 15 de fevereiro de 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 1988. Disponível em: < https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 20 de março de 2024.

BRASIL. **Crimes digitais: o que são, como denunciar e quais leis tipificam como crime?** Conselho Nacional de Justiça, 2018. Disponível em: <https://www.cnj.jus.br/crimes-digitais- o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime/ >. Acesso em 15 de fevereiro de 2024.

BRASIL. Decreto-lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Brasília, DF: Presidência da República, 1940. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm> . Acesso em 15 de março de 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais** (LGPD). Brasília, 2018. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 25 de março de 2024.

BRASIL. **O que é a LGPD?** Ministério Público Federal, 2021. Disponível em: <https://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd >. Acesso em 15 de março de 2024.

BRASIL. **Você sabe o que é a Lei Geral de Proteção de Dados Pessoais e para que ela**

serve? Ministério da Integração e do Desenvolvimento Regional. 2023. Disponível em:<https://www.gov.br/sudeco/pt-br/assuntos/noticias/2023/voce-sabe-o-que-e-a-lei-geral- de-protecao-de-dados-pessoais >. Acesso em 24 de março de 2024.

BUGHUNT**. Crimes cibernéticos: como eles acontecem e como evitá-los?** 2023. Disponível em:<https://blog.bughunt.com.br/crimes-ciberneticos/>. Acesso em 15 de março de 2024.

EL DEBS, A.I. **Dos crimes contra a honra na seara digital**. Consultor jurídico, 2022. Disponível em:<https://www.conjur.com.br/2022-set-03/aline-iacovelo-crimes-honra-seara- digital/ >. Acesso em 15 de março de 2024.

FACHINI, Tiago. **Marco Civil da Internet: o que é e como funciona?** ProJuris, 2022. Disponível em:<https://www.projuris.com.br/blog/marco-civil-da-internet/ >. Acesso em 20 de março de 2024.

GARCIA, Rafael de Deus. **Os direitos à privacidade e à intimidade: Origem, distinção e dimensões.** Revista da Faculdade de Direito do Sul de Minas, Pouso Alegre, v.34, n.1:1-26, jan./jun.2018. Disponível em:<https://revista.fdsm.edu.br/index.php/revistafdsm/article/view/257/214 >. Acesso em 10 de março de 2024.

HOSTDIME. **ataques de ransomware no setor da saúde: entensa os desafios.** Disponível em: <https://www.hostdime.com.br/ataques-de-ransomware-no-setor-da-saude-entenda-os- desafios/ >. Acesso em 05 de março de 2024.
HOSTINGER TUTORIAIS. **A história da Internet e suas tecnologias**- Da guerra Fria a 2023. 2023. Disponível em<https://www.hostinger.com.br/tutoriais/a-historia-da-internet >. Acesso em 10 de março de 2024.

Jesus, Damásio de. **Manual de crimes informáticos** / Damásio de Jesus, José Antonio Milagre. – São Paulo : Saraiva, 2016.

JORNAL DA USP. **Brasil sofreu mais de 100 bilhões de tentativas de ataques cibernéticos no último ano.** 2023. Disponível em:<https://jornal.usp.br/radio-usp/brasil- sofreu-mais-de-100-bilhoes-de-tentativas-de-ataques-ciberneticos-no-ultimo-ano/ >. Acesso em 15 de março de 2024.

MARGENTA, Matheus. **O que é liberdade de expressão**. BBC News Brasil, 2022. Disponível em: <https://www.bbc.com/portuguese/geral-62550835 >. Acesso em 10 de março de 2024.

MENDES, Rafael Pereira da Silva. "**Liberdade de expressão**"; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/sociologia/liberdade-de-expressao.htm. Acesso em 26 de março de 2024.

NAZAR, Susanna**. Casos de pedofilia virtual se multiplicam no Brasil com os avanços da inteligência artificial.** Jornal da USP. 2023. Disponível em:<https://jornal.usp.br/atualidades/casos-de-pedofilia-virtual-se-multiplicam-no-brasil-com-os-avancos-da-inteligencia-artificial/#:~:text=Atualmente%2C%20n%C3%A3o%20existe%20na%20legisla%C3%A7%C3%A3o,Privacidade%20e%20Prote%C3%A7%C3%A3o%20de%20Dados>. Acesso em 15 de fevereiro de 2024.

NEON. **Crimes cibernéticos: exemplos, o que diz a lei e como prevenir.** 2023. Disponível em: <https://neon.com.br/aprenda/seguranca-digital/crimes-ciberneticos/>. Acesso em 20 de fevereiro de 2024.

ONE TELECOM. **O que podemos considerar como benefícios da internet.** 2021. Disponível em: <https://onetelecom.net.br/quais-sao-os-reais-beneficios-da-internet/>. Acesso em 25 de fevereiro de 2024.

PEREIRA, E.A. **Reflexões sobre o crime de invasão de dispositivo informático e o PL 879/22**. Consultor Jurídico, 2023. Disponível em: <https://www.conjur.com.br/2023-mai- 05/emanuela-pereira-invasao-dispositivo-informatico-pl-879/ >. Acesso em 20 de março de 2024.

POSITIVO TECNOLOGIA**. Pontos positivos e negativos da tecnologia para a sociedade atual.** 2019. Disponível em<https://www.meupositivo.com.br/panoramapositivo/tecnologia- para-a-sociedade-atual/ >. Acesso em 5 de março de 2024.

RAMOS, Rahellen. **O que é o Marco Civil da internet?** Politize, 2021. Disponível em: <https://www.politize.com.br/marco-civil-da-internet/ >. Acesso em 26 de março de 2024.

Teixeira, Tarcisio. Direito Digital e Processo Eletrônico / Tarcisio Teixeira. – 6. ed. – São Paulo : SaraivaJur, 2022.

TELECO. Crime digital: cibercrime- Uma realidade e suas motivações. 2024. Disponível em: <https://www.teleco.com.br/tutoriais/tutorialalcrimedig/pagina_3.asp >. Acesso em 20 de março de 2024.