Centro Universitário do Planalto Central Apparecido dos Santos - UNICEPLAC
Curso de Direito
Trabalho de Conclusão de Curso

Crimes cibernéticos: a dificuldade da aplicação do Código Penal diante da evolução dos crimes cibernéticos

Gama-DF
2024

PALOMA LOURRANY ALVES SILVA

Crimes cibernéticos: a dificuldade da aplicação do Código Penal diante da evolução dos crimes cibernéticos

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Direito pelo Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac.

Orientador: Prof Me. João de Deus Alves de Lima

Gama-DF
2024

PALOMA LOURRANY ALVES SILVA

Crimes cibernéticos: a dificuldade da aplicação do Código Penal diante da evolução dos crimes cibernéticos

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Direito pelo Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac.

Gama-DF, 29 de outubro de 2024.

Banca Examinadora

Prof. Me. João de Deus Alves de Lima
Orientador

Profa. Me. Caroline Lima Ferraz
Examinador

Prof. Me Antônio Róger Pereira de Aguiar
Examinador

Crimes cibernéticos: a dificuldade da aplicação do Código Penal diante da evolução dos crimes cibernéticos

Paloma Lourrany Alves Silva[1]

Resumo:
Este artigo tem como objetivo abordar acerca da dificuldade da aplicação do Código Penal diante da evolução dos crimes cibernéticos. A metodologia usada no artigo foi o método indutivo. A doutrina descreve crimes cibernéticos como qualquer ato em que é realizado por meio de computadores, meios de tecnologia da informação para cometer um ato ilícito, sendo o computador ou os meios tecnológicos objetos do crime. O resultado obtido neste artigo é que os crimes cibernéticos estão presentes em toda a sociedade e as tecnologias continuam a evoluir. Contudo, é preciso que a sociedade junto com o governo e empresas adotem ações para proteger os sistemas e informações críticas. Além disso, devem desenvolver abordagens que consigam identificar os cibercriminosos e responsabilizar os responsáveis pelos crimes cibernéticos. É imperativo a precaução e segurança contra esses crimes, e a necessidade de uma abordagem multidisciplinar que inclua segurança cibernética, regulamentação atualizada e cooperação internacional voltada no treinamento e qualificação de agentes qualificados em combater os crimes cibernéticos, para atacar essa ameaça transnacional.

Palavras-chave: crimes cibernéticos; segurança cibernética; cibercriminosos.

Abstract:
This article aims to address the difficulty of applying the Penal Code in light of the evolution of cyber crimes. The methodology used in the article was the inductive method. Doctrine describes cybercrime as any act committed through computers or information technology to commit an illicit act, with the computer or technological means being objects of the crime. The result obtained in this article is that cybercrimes are present throughout society, and technology continues to evolve. However, it is necessary for society, along with the government and companies, to adopt actions to protect critical systems and information. In addition, they should develop approaches capable of identifying cybercriminals and holding those responsible for cybercrimes accountable. Precaution and security against these crimes are imperative, as is the need for a multidisciplinary approach that includes cybersecurity, updated regulation, and international cooperation focused on the training and qualification of agents skilled in combating cybercrimes to address this transnational threat.

Keywords: Cyber crimes; cybersecurity; cybercriminals.

1. INTRODUÇÃO

O presente artigo tem como objetivo abordar acerca da dificuldade da aplicação do Código Penal diante da evolução dos crimes cibernéticos. Com o desenvolvimento da tecnologia, as pessoas estão sempre conectadas através da *internet* ao mundo, deixando-as mais vulneráveis aos

[1]Graduanda do Curso Direito, do Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac. E-mail: palomalvesplas@gmail.com.

crimes eletrônicos que hoje representam uma modalidade nova de crime aplicado por meio virtual. Além disso, os crimes na modalidade virtual têm natureza transcendental, podendo o criminoso atuar de qualquer local do país, o que aumenta o alcance dos crimes, antes restritos a uma quantidade limitada de indivíduos.

O estudo busca abordar a relevância da criminalização dos crimes cibernéticos, contextualizando acerca da ausência de legislação no sistema jurídico brasileiro e em especial o Código Penal que não abrange as condutas ilícitas que ocorrem no mundo virtual, trazendo insegurança jurídica e social. A elaboração do estudo foi composta por revisão bibliográfica, com o uso de doutrinas renomadas pelo Direito Penal Brasileiro, como Guilherme de Souza Nucci, Rogério Greco, Fernando Capez, Patrícia Peck Pinheiro, Damásio de Jesus, José Antônio Milagre, Marcelo Xavier de Freitas Crespo, dentre outros. Além disso, foram utilizadas jurisprudências, leis codificadas, trabalhos científicos, artigos, monografias e legislações internacionais que tipificam os crimes cibernéticos e o método usado nesse estudo foi o método indutivo.

Esse tema é importante devido ao impacto que o fenômeno dos crimes cibernéticos possui na sociedade, ou seja, sua grande relevância num contexto social que influencia na vida das pessoas, levando-se em consideração que esse tipo de acontecimento está sujeito a acontecer com qualquer pessoa, pois a *internet* é utilizada pela sociedade para realizar tarefas cotidianas como efetuar transações bancárias através de aplicativos de *internet banking*[2]. Dessa maneira, nesses dispositivos informáticos são armazenadas as informações dos seus usuários, podendo ser informações sigilosas, que ao serem violados podem gerar diversos prejuízos.

Crimes cibernéticos, como o próprio nome sugere, é uma conduta criminosa que envolve o uso de computadores, redes de comunicação ou dispositivos eletrônicos para realização de atividades criminosas. A doutrina define crimes cibernéticos como qualquer ato em que é utilizado como meio os computadores, meios de tecnologia da informação para cometer um ato ilícito, sendo o computador ou os meios tecnológicos objetos do crime.

A estrutura do estudo é formada por quatro capítulos, que trazem um cenário geral acerca dos crimes cibernéticos, o primeiro capítulo será realizado uma análise do conceito do crime cibernético, além de abordar a evolução histórica desses delitos. Em seguida, no segundo, será abordado as principais espécies de crimes cibernéticos: crimes contra a honra nas redes sociais, estelionato virtual e o *cyberstalking*. Já no terceiro capítulo serão apresentadas as legislações para os crimes cibernéticos, será tratado os marcos legais, como a Convenção de Budapeste (Hungria, 2001), a Lei n° 12.965/2014 o marco civil da *internet*, Lei nº 12.737/2012 popularmente conhecida como Lei da Carolina Dieckmann e a Lei n° 13.709/2018, a Lei geral de proteção de dados. Por fim, o quarto capítulo abordará os desafios para a aplicação das legislações pelo ordenamento jurídico.

A doutrina elenca várias nomenclaturas utilizadas nas pesquisas acadêmicas sobre os crimes cibernéticos, entre as quais destacamos os crimes de computador, crime via *internet*, crime informático, crime praticado por meio da *internet*, crime praticado por meio da informática, crime tecnológico, crime da *internet*, crime digital, *cyber* crimes, *info* crimes etc.

Para efeito deste estudo, o artigo adotará o conceito de crime cibernético, abrangendo as condutas delitivas que se utilizam ou que se voltar contra os dispositivos de comunicação ou eletrônicos. Adotará o conceito de crime cibernético como uma conduta criminosa que envolve o uso de computadores, redes de comunicação ou dispositivos eletrônicos para realização de atividades criminosas, bem como delitos que envolvem a fraude de equipamentos tecnológicos,

[2] O termo *internet banking* é utilizado para realizar transações bancárias ou gerenciar contas financeiras utilizando a *internet*.

sistemas de informação ou banco de dados.

A hipótese que será verificada nesse artigo é que o Código Penal não abrange todos os crimes cibernéticos existentes na atualidade, apesar de já existirem leis que tipificam os crimes virtuais, os *cybers* criminosos são habilidosos e a cada vez evoluindo seus métodos criminosos. O Código Penal deve evoluir conforme os crimes evoluem.

2. CONCEITO DE CRIMES CIBERNÉTICOS

A regulação dos crimes no mundo virtual é um tema muito complexo e delicado. Isso porque sem a devida tipificação dos crimes cibernéticos, tem-se o risco de punir uma pessoa inocente. Além disso, sabe-se que na forense digital[3] as ‘‘testemunhas máquinas’’ não conseguem distinguir culpa de dolo. O computador não pode trazer informações sobre o contexto da situação, muito menos distinguir se houve intenção ou não do agente cometer o delito. Desse modo, um exemplo, é a tentativa de tipificar o crime de um arquivo com *vírus* para um *e-mail*. As pessoas, muitas vezes, enviam o arquivo sem saber que se tratava de um arquivo malicioso. (Pinheiro, 2023, p. 386)

A doutrina apresenta diversas nomenclaturas que são utilizadas em trabalhos sobre os crimes que ocorrem no meio virtual, entre elas: crime de computador, crime via *internet*, crime informático, crime praticado por meio de *internet*, crime praticado por meio de informática, crime tecnológico, crime da *internet*, crime digital, *cyber crimes*, *info* crimes, entre outras. (Crespo, 2011, p. 20) Quando se fala de meios informáticos, deve-se compreender os *hardwares* e *softwares* de computadores, *tablets*, *smartphones*, entre outros dispositivos que podem ser utilizados para praticar a conduta delitiva.

Além disso, Alexandre Júnior define crimes cibernéticos como qualquer ato em que é utilizado como meio os computadores, meios de tecnologia da informação para cometer um ato ilícito, sendo o computador ou os meios tecnológicos objetos do crime. O *cibercrime* está ligado ao fenômeno da criminalidade informacional, que envolve condutas que violam direitos fundamentais, por meio da utilização de informática para a prática criminosa. (Alexandre Júnior, 2019, p. 3)

Desse modo, neste artigo, será adotada a denominação de crime cibernético, pois essa denominação abrange todas as tecnologias e práticas criminosas. Reconhece-se, entretanto, a necessidade de uma avaliação técnico-jurídica. Ainda assim, é importante ressaltar que essa expressão não satisfaz plenamente a função dogmática de integração. Por fim, esclarece-se que, apesar de tecnicamente o termo mencionado refere-se aos ilícitos praticados com uso da telemática, a justificativa para sua preferência é que o termo *cibercrime* foi utilizado no Acordo Internacional do Conselho da Europa, em novembro de 2001. (Crespo, 2011, p. 21)

Desse modo, os crimes cibernéticos são caracterizados como crimes de fato típico, antijurídico e culpável, ocorrendo quando são cometidos contra ou através do uso de sistema cibernético. (Cavalcanti Neto, 2023, p. 7)

Com base nessa definição, é possível classificá-los como crimes cibernéticos próprios e crimes cibernéticos impróprios. Os primeiros são aqueles que só podem ser praticados na informática, ou seja, a execução e a consumação do crime ocorrem nesse meio. Trata-se de tipos novos de crimes, nos quais o bem jurídico tutelado é a informática. Esses crimes são cometidos contra os dados das vítimas que utilizam computadores, *tablets*, *smartphones*, entre outros

[3] Conhecida como computação forense, a forense digital é a prática de coletar, preservar e analisar evidências digitais de maneira que possa ser apresentado em juízo.

dispositivos. Essas condutas são praticadas por *hackers*[4], que invadem sistemas para modificar, alterar, inserir dados ou informações falsas, afetando diretamente os *softwares* dos computadores. A invasão pode ocorrer através do uso de *pen drives*, *e-mails* com arquivos infectados baixados de sites não confiáveis, que contêm *vírus*[5]. Esses *vírus* podem danificar diversos programas e arquivos, e, em alguns casos, é necessário formatar os dispositivos para remover o *malware*. (Tormen, 2018, p. 13)

Nos crimes cibernéticos impróprios, trata-se de crimes já tipificados no Código Penal, que violam bens jurídicos comuns e ferem a dignidade da pessoa humana, exemplos incluem crimes contra a honra através de publicação na *internet*, entre outros que ocorrem no meio informático. (Tormen, 2018, p. 13)

Essa classificação diferencia os atos ilícitos que foram praticados por meio do sistema cibernético daqueles praticados contra esse sistema. Por esse motivo, é importante ter cautela ao adaptar as leis existentes aos delitos praticados através da *internet*, bem como reconhecer que existem situações que requerem tutela específica, com a criação de novas leis. (Cavalcanti Neto, 2023, p. 7)

2.1 Evolução histórica dos crimes cibernéticos

Desde tempos remotos até os dias atuais, o ser humano sempre se empenhou em desenvolver máquinas e ferramentas que o auxiliassem em suas atividades cotidianas. (Crespo, 2011, p. 12) Os primeiros ataques cibernéticos representam os primeiros passos em direção a uma era digital que se desdobraria em uma paisagem virtual complexa e, por vezes, perigosa. Os primeiros relatos de abusos no uso de computadores surgiram na década de 1960, com manipulação de dados, sabotagem, espionagem e uso ilegal dos sistemas de computadores. Na maioria das vezes, esses crimes eram cometidos por especialistas que utilizam a inteligência para arquitetar planos relacionados à aplicação de golpes em instituições financeiras. (Maia; Costa, 2023, p. 7)

Um dos primeiros crimes cibernéticos registrados, é o caso do *Wabbit*. Trata-se de um programa autorreplicante que se espalhava de sistema para sistema. Seu propósito não era malicioso, mas sim demonstrar a capacidade de replicação de código. (Maia; Costa, 2023, p. 7)

Os primeiros ataques cibernéticos marcam o início de uma jornada que levou a uma compreensão mais profunda dos sistemas digitais. No entanto, também destacaram a necessidade premente de uma segurança cibernética robusta para proteger sistemas e informações sensíveis em um mundo cada vez mais interconectado. (Maia; Costa, 2023, p. 8)

Neste contexto, o crime cibernético não é uma questão exclusivamente contemporânea, uma vez que remonta aos tempos remotos, quando o meio tecnológico era mais distante e inacessível para a maioria das pessoas. É importante para compreender que esses crimes foram inicialmente praticados na década de 60, nos Estados Unidos da América. (Maia; Costa, 2023, p. 7)

Dessa forma, a doutrina apresenta divergências sobre o primeiro delito cibernético. De acordo com Jesus e Milagre, há diferentes opiniões sobre esse assunto:

> Para alguns, o primeiro delito informático teria ocorrido no âmbito do MIT (*Massachusetts Institute of Technology*), no ano de 1964, onde um aluno de 18

[4] *Hackers* são indivíduos com habilidades avançadas em informática e programação, que utilizam seus conhecimentos para explorar sistemas de computadores e redes.

[5] O vírus é um tipo de *malware* (*software* malicioso) que se propaga entre computadores e redes com a intenção de causar danos ou roubar informações. Os vírus são projetados para se replicar e espalhar, geralmente anexando-se a arquivos ou programas legítimos

> anos teria cometido um ato classificado com *cibercrime*, tendo sido advertido pelos superiores. Outros ainda referenciam o primeiro caso de que se tem notícia sobre *hacking* no ano de 1978, na Universidade de Oxford, onde um estudante copiou de uma rede de computadores uma prova. Uma invasão seguida de uma cópia. Até essa data não existia lei sobre crimes informáticos nos Estados Unidos. A Flórida, no mesmo ano, foi o primeiro Estado americano a formular leis sobre informática. (Jesus; Milagre, 2016, p. 9)

Nos anos 70, o termo *hacker* começou a ser mencionado, com o surgimento de crimes como invasão de sistemas e furto de *software*. No entanto, foi a partir da década de 1980 que novos casos de pirataria de programas, manipulação de valores nos caixas eletrônicos e abusos nas telecomunicações começaram a ser detectados, revelando para o público geral a vulnerabilidade da sociedade da informação. Essa vulnerabilidade levou a debates sobre a necessidade de se priorizar a segurança e de tentar controlar tais condutas prejudiciais na sociedade. (Henriques; Gonçalves, 2024, p. 4)

Em decorrência dessa mudança na percepção pública e científica dos crimes cibernéticos, como indicam os dados informados pela *Federal Bureau of Investigation* (FBI) nos Estados Unidos mostraram que os crimes cibernéticos denunciados totalizaram prejuízos de U$ 3,5 bilhões (cerca de R$ 15 bilhões), somente em 2019. Isso levou a tipificar legalmente as condutas relacionadas à informática. (Pinheiro, 2024, p. 387).

Uma das principais motivações por trás dos crimes cibernéticos é o lucro financeiro. Os criminosos cibernéticos veem a *internet* como um meio de obter ganhos substanciais, engajando-se em atividades como fraudes financeiras, como a clonagem de cartões de crédito, extorsão por meio de *ransomware* e esquemas de *phishing*, destinados a roubar informações financeiras de vítimas desavisadas. (Maia; Costa, 2023, p. 8)

Nesta perspectiva, temos o caso ocorrido em Los Angeles:

> Um dos casos internacionais que mais marcaram a história dos crimes cibernéticos, em sua fase inicial, foi o caso *Equity Founding Life INsurance Company*, em Los Angeles. Este caso configurou-se em uma das maiores fraudes de computadores já mencionada, esta situação se caracterizou por ter chegado à marca de 2 bilhões de reais. (Maia; Costa, 2023, p. 9)

Desse modo, além do objetivo monetário, o crime cibernético pode impactar significativamente o psicológico das vítimas. Os criminosos utilizam o meio tecnológico para instigar e coagir as vítimas a realizarem determinados atos. Um caso de extrema relevância no Brasil relacionado a essa temática foi o caso da Baleia Azul[6].

Este não foi o primeiro caso de crimes cibernéticos envolvendo aspectos psicológicos. A imprensa divulgou que uma adolescente de 16 anos, de Vila Rica (MT), cometeu suicídio, além do caso de um jovem de 19 anos, de Pará de Minas (MG). Ambas as mortes estão relacionadas ao jogo da Baleia Azul. (Conselho Federal da Ordem dos Advogados, 2017, n.p.) Este jogo instigava os jovens, de forma virtual, a participar de fases que, ao final levavam ao suicídio do participante. Isso alarmou os agentes voltados responsáveis por analisar a criminalidade cibernética no Brasil. (Maia; Costa, 2023, p. 9)

[6] O jogo da Baleia Azul é um fenômeno que surgiu nas redes sociais e se tornou amplamente conhecido por suas práticas perigosas. Trata-se de um desafio virtual que envolve uma série de tarefas atribuídas aos participantes ao longo de 50 dias. Essas tarefas começam com atividades inofensivas, mas gradualmente evoluem para ações autodestrutivas e perigosas, como a automutilação. O desafio final, supostamente, é o suicídio.

Os ataques cibernéticos também são motivados por razões políticas. Os grupos de *hackers*, chamados de hacktivistas[7] e os governos frequentemente realizam ciberataques para obter informações estratégicas, realizar espionagem industrial, influenciar eleições ou promover agendas políticas. No contexto atual, a busca por informações úteis e verídicas tornou-se uma motivação central para os ciberataques. A espionagem cibernética é conduzida por governos, grupos de *hackers* e empresas interessadas em obter dados confidenciais, como a propriedade intelectual e disseminação de informações de *fake News*[8]. (Maia; Costa, p. 9)

Portanto, à medida que a tecnologia avança, torna-se crucial que a sociedade, governos e empresas adotem medidas para proteger as informações dos cidadãos e desenvolver estratégias para identificar e responsabilizar os autores de crimes cibernéticos. Além disso, a prevenção e proteção contra esses delitos exigem uma abordagem multidisciplinar, que inclui segurança cibernética, legislação adequada e a cooperação internacional para combater as ameaças. (Maia; Costa, 2023, p. 10)

3. PRINCIPAIS ESPÉCIES DE CRIMES CIBERNÉTICOS

Variadas são os tipos de espécie de crimes realizados no ambiente virtual. Todavia, ao abordar os crimes cibernéticos comuns, refere-se àqueles que são praticados quando o invasor cibernético utiliza da tecnologia como um meio para praticar o fato típico, a maioria dos crimes que acontecem no ambiente virtual ocorrem também na vida real.

Desse modo, nota-se que o usuário do ambiente virtual se sente seguro pelo anonimato de segurança, tornando ainda mais propício para cometer crimes virtuais. A seguir serão analisadas condutas criminosas praticadas no contexto eletrônico, como os crimes contra a honra nas redes sociais, o estelionato virtual e o *cyberstalking*.

3.1 Crimes contra a honra nas redes sociais

Com a ampliação do acesso à *internet* e a evolução das redes sociais, como *Facebook*, *Instagram*, *Twitter* e Whatsapp, a disseminação de informações se tornou mais abrangente. A expansão da *internet* alterou totalmente a forma com que as pessoas interagem. (Castro; Nazareth; Marques; Ferreira, 2021, p. 2) Como consequência, os crimes contra a honra, antes restritos ao espaço físico, passaram a ocorrer também na esfera digital. Dessa forma, o potencial de propagação desses crimes, previstos no Código Penal de 1940, aumentou, prejudicando a integridade moral e comprometendo a honra das vítimas. (Brasil, 1988, n.p.)

No contexto da *internet*, tornou-se comum a ocorrência de ataques, agressões, vandalismo e até mesmo crimes envolvendo pessoas físicas e jurídicas em ambientes eletrônicos, onde as únicas testemunhas são as máquinas. (Pinheiro, 2021, p. 417)

A honra é um bem jurídico protegido pela Constituição Federal do Brasil, considerada um direito fundamental, conforme o artigo 5º, inciso X: ‘‘são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral

[7] Hacktivistas são indivíduos ou grupos que utilizam técnicas de *hacking* para promover agendas políticas, sociais ou ideológicas. Combinando os termos hacker e ativista, eles empregam suas habilidades técnicas para realizar ações que vão desde ataques de negação de serviço (DDoS) a invasões de sistemas, visando divulgar informações, protestar contra instituições ou chamar a atenção para determinadas causas.

[8] *Fake news* são notícias falsas ou enganosas criadas para parecer verdadeiras.

decorrente de sua violação’’. Já que a honra está intrinsecamente ligada à dignidade da pessoa humana, pois diz respeito diretamente à reputação do indivíduo. (Brasil, 1988, n.p.)

O direito à intimidade e à própria imagem formam a proteção constitucional à vida resguardando um espaço íntimo intransitável por intromissões ilícitas de outrem. Além disso, a proteção constitucional do inciso X do artigo 5º, trata-se tanto de pessoas físicas como de pessoas jurídicas, abarcando, inclusive, a proteção de imagem frente aos meios de comunicação em massa, como televisão, rádio, dentre outros. (Moraes, 2023, p. 77)

Além disso, com o significativo aumento do desenvolvimento tecnológico ocorrido nas últimas décadas, atrelado a redução de custos no custo final de aparelhos como *laptops*, *tablets*, *smartphones*, computadores pessoais, dentre outros. Propiciaram um aumento progressivo de usuários na rede mundial de computadores, a *internet*. De acordo com dados das Nações Unidas, o Brasil está em 4º lugar em números de internautas, com mais de 120 milhões de usuários conectados à rede *online*. (Tribunal de Justiça do Rio de Janeiro, 2019, n.p.)

Ademais, o índice de *smartphones* no país já passou da quantidade habitantes, sendo 236 milhões de aparelhos para 210 milhões de habitantes, de acordo com os dados de 2018. (Tribunal de Justiça do Rio de Janeiro, 2019, n.p.) As principais redes sociais, são o *Twitter*, *Facebook* e *Instagram*, essas são redes utilizadas de forma significativa para o cometimento desses crimes como: injúria, calúnia e difamação. (Castro; Nazareth; Marques; Ferreira, 2021, p. 5)

O Código Penal prevê três tipos de crimes contra a honra nos artigos 138, 139 e 140, sendo eles: Calúnia, difamação e injúria. Quando esses crimes são cometidos por meio de redes sociais, a pena é aumentada, conforme dispõe o artigo 141, §2º do Código Penal: ‘‘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, n.p.)

Um dos principais e mais comuns crimes cibernéticos é o crime de difamação, previsto no artigo 139 do Código Penal. Esse crime consiste em divulgar conteúdos que ofendam a reputação de uma pessoa, resultando na perda do respeito social, independentemente da veracidade das alegações. Com o objetivo de atingir a honra de outrem, causando danos à sua vida pessoal e social. (Brasil, 1940)

É importante destacar que, no crime de calúnia há a imputação de um fato criminoso a alguém, a pessoa que atribui a acusação sabe que é falsa, (Crespo, 2011, p. 25) previsto no artigo 138 do Código Penal Brasileiro. Nesse crime, é necessário que se atribua a vítima um fato determinado previsto em lei como crime e que essa atribuição é falsa. Contudo, caso o criminoso esteja agindo de boa-fé, supondo ser verdade, a intenção será excluída. Desse modo, o crime será excluído. Um exemplo de calúnia, é espalhar *e-mails*, *post* nas redes sociais que uma pessoa abusou sexualmente de outra, ou desvio valores financeiros de uma empresa, caracterizam como crime de calúnia. (Crespo, 2011, p. 25)

Ademais, o crime de difamação, está previsto no artigo 139 do Código Penal, e é praticado por meio de publicações virtuais criminosas. Ocorre o crime de difamação quando há uma atribuição de um fato específico, mas que não é classificado como crime. A difamação ocorre quando é atribuído um fato ofensivo à reputação da vítima, desvalorizando publicamente. A lei não necessita que a atribuição falsa seja de fato desonrosa, podendo caracterizar o crime com a afirmação do fato verídico. (Crespo, 2011, p. 25)

Em geral, os crimes contra a honra devem ser denunciados pela vítima em uma delegacia. Como a lei determina a pena máxima de dois anos para esses delitos, essas ações tramitam nos Juizados Especiais Criminais. No entanto, é importante considerar a complexidade da apuração dos

crimes cibernéticos, pois é muito fácil para o criminoso apagar os vestígios do crime, como, por exemplo, mensagens ofensivas em redes sociais. (Nunes, 2023, p. 14)

O crime de injúria é um crime que viola a honra subjetiva, previsto no artigo 140 do Código Penal Brasileiro tem como objetivo atribuir qualidades negativas a uma pessoa, geralmente por meio de insultos, xingamentos, atacando a moral da vítima e ofendendo sua dignidade e decoro. O crime se consuma quando a vítima toma conhecimento do fato, sendo desnecessário que outras pessoas também tenham conhecimento. (Crespo, 2011, p. 25)

Portanto, as leis sobre os crimes contra a honra foram estabelecidas pelo Código Penal de 1964, em um contexto social diferente do de 2020. Desse modo, é necessário que os dispositivos legais reflitam a realidade atual e sejam suficientes para atender os problemas sociais. A ausência de normas específicas para crimes cometidos na *internet* e a utilização de normas genéricas sobre crimes contra a honra gera uma ineficácia para punir esses delitos, levando à impunidade dos autores; (Castro; Nazareth; Marques; Ferreira, 2021, p. 11)

3.2 Estelionato virtual

O Código Penal Brasileiro, em seu capítulo V, artigo 171 tipifica o crime de estelionato: ‘‘Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento’’. (Brasil, 1940, n.p.) Para tipificar o crime estelionato, são necessários quatro requisitos essenciais: a) obtenção de vantagem ilícita; b) causar prejuízo a outrem; c) uso de meio de ardil ou artimanha; d) enganar alguém ou levá-lo ao erro. Portanto, a ausência de qualquer um desses requisitos impede a caracterização do crime de estelionato. Além disso, no crime de estelionato, o criminoso não faz uso de violência ou grave ameaça. (Gonçalves; Henriques, 2024, p. 7)

O estelionato, como categoria de crime, foi transposto para os ambientes virtuais devido aos avanços ocorridos pela tecnologia e pela criação de diversos dispositivos tecnológicos que facilitaram a interação de seus usuários em seu dia a dia. Esse crime, com sua notável rapidez, adaptou-se à nova realidade virtual, utilizando meios eletrônicos para a prática de diversos delitos, especialmente o estelionato virtual. (Machado, 2022, p. 2)

Primeiramente, o estelionato virtual é aquele em que o sujeito, utilizando de equipamentos tecnológicos e de acesso à rede digital, pratica condutas tipificadas no artigo 171 do Código Penal. (Garutti; Brito, 2023, n.p.) Nesse sentido, com o objetivo de combater esse crime, entrou em vigor a Lei nº 14.155/2021[9] que agravou as penalidades para os crimes de furto e estelionato praticados por meio virtual. (Machado, 2022, p. 2)

No ambiente virtual, o estelionato ocorre quando o agente induz ou mantém a vítima em erro, com o objetivo de obter vantagem ilícita, seja para si ou para terceiros. (Gonçalves; Henriques, 2024, p. 8) Na maioria dos casos, a participação da vítima é feita de boa-fé, sem a consciência de que foi enganada pelo criminoso. A finalidade é levar a vítima a fornecer de forma espontaneamente seus dados pessoais, permitindo que os criminosos obtenham benefícios em nome da vítima, utilizando seus dados pessoais. (Nunes, 2023, p. 14) Além disso, os criminosos não atuam sozinhos, e para que seja configurado como estelionato, é necessário que a vítima

[9] Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato

entregue a vantagem de forma espontânea ao criminoso. Caso contrário, a ação seria classificada como outra modalidade de crime, como extorsão ou roubo.

No entanto, observa-se que, em alguns casos, após a realização das negociações, o resultado concreto pretendido pela vítima pode ser igualmente imoral ou ilícito. Mesmo nessas situações, o crime de estelionato também se configura. Portanto, no tipo penal, o crime de estelionato não exige qualquer qualidade, tanto o sujeito ativo, como o passivo, pode figurar como autor do crime ou podendo ser a vítima, sendo essencial, para caracterizar o crime o preenchimento dos elementos, seja eles: vantagem ilícita, fraude e prejuízo alheio. (Almeida, 2023, p. 19)

Entre os crimes cibernéticos, o crime de estelionato por meio digital lidera as ocorrências anotando notáveis 200.322 casos no ano de 2022. Contudo, é importante salientar que esse número poderia ser mais elevado, pois exclui os dados de determinados estados. Além disso, outro ponto é o estudo das taxas de estelionato eletrônico por 100 mil habitantes. Nesse contexto, os estados de Santa Catarina, Distrito Federal e Espírito Santo apresentam os maiores índices, fortalecendo a importância de fortalecer a segurança cibernética nessas localidades. *(International IT*, 2023, n.p.)

Desse modo, é evidente que o crescimento dessa modalidade de crime se deve à falsa sensação de que o ambiente virtual é um ‘‘território sem lei’’. (Machado, 2022, p. 3) No entanto, essa percepção não reflete a realidade, pois, embora ainda de forma tímida e gradual, as autoridades responsáveis estão empenhadas em punir os criminosos e reprimir os crimes praticados no ambiente digital. (Machado, 2022, p. 3)

Ademais, uma das principais modalidades de crimes praticadas por estelionatários virtuais é atualmente denominada como clonagem do *whatsapp*[10]. Desde a criação dos aplicativos de comunicação, os métodos utilizados para executar fraudes têm sido modificados, apresentando várias variações na execução desse crime. (Gonçalves; Henriques, 2024, p. 13)

Para que esse crime ocorra, o fraudador precisa ter acesso ao número de telefone utilizado pela vítima no aplicativo *whatsapp*. Com o telefone da vítima em mãos, o transgressor tenta ingressar na conta do *whatsapp* pertencente à vítima. Por meio desse acesso ilícito, o criminoso avança para a próxima do crime: a obtenção de benefício financeiro indevido. O criminoso se passa pela vítima, interagindo com familiares, cônjuges, amigos, clientes, entre outros, e solicita dinheiro para as novas vítimas, alegando problemas com o cartão de crédito, dificuldades bancárias ou que ultrapassou o limite diário para pagamento de boletos. Assim, as novas vítimas realizam a transação, acreditando na promessa de reembolso. (Gonçalves; Henriques, 2024, p. 14)

Dessa forma, a pessoa prejudicada, acreditando estar conversando com um conhecido, efetua o pagamento do boleto ou faz a transferência bancária para a conta do fraudador, concluindo mais um estelionato virtual. O golpe só é descoberto quando o titular do *whatsapp*, a primeira vítima, consegue entrar em contato com as demais vítimas envolvidas. (Gonçalves; Henriques, 2024, p. 14) Portanto, destaca-se a fragilidade na identificação do indivíduo, tendo em vista que nessa espécie de delito, em grande parte, os estelionatários se camuflam no anonimato para realização e consumação da prática, o que intensifica a vulnerabilidade das investigações no meio virtual. (Garutti; Brito, 2023, n.p.)

3.3 *Cyberstalking*

[10] A clonagem do *whatsapp* é um golpe em que criminosos duplicam a conta de um usuário, acessando suas mensagens e contatos para aplicar fraudes, geralmente pedindo dinheiro em nome da vítima.

O termo c*yberstalking* deriva da palavra s*talking*[11], que pode ser definido como o ato de perseguir alguém, de forma contínua e reiterada, ameaçando sua integridade física e psicológica, restringindo sua liberdade de locomoção ou invadindo sua privacidade ou liberdade. Desse modo, *cyberstalking* é a prática de perseguir alguém *online* de forma persistente e indesejada no ambiente *online*. Essa perseguição pode manifestar-se de várias formas, incluindo ameaças, difamação, assédio sexual, calúnia, ações de intimidação ou tentativas de influenciar a vítima. (Ferreira, 2024, p. 25)

Uma das distinções entre a perseguição comum, conhecida como *stalking,* e a perseguição cibernética está na proximidade geográfica entre o criminoso e a vítima. No caso do *stalking*, o perseguidor necessita de tempo e recursos para deslocamento, seguindo a vítima em todos os locais, como em casa, na faculdade, ou na academia. O *cyberstalking* é facilitado pelo mundo virtual, exigindo o uso de energia e de computadores para sua realização. (Ferreira, 2024, p. 24) Desse modo, o ofensor cibernético pode assediar a vítima de qualquer lugar do mundo, precisando apenas ter acesso a um dispositivo conectado à *internet*.

O crime de *stalking* foi adicionado ao Código Penal Brasileiro por meio da Lei nº 14.132/2021, que incluiu o artigo 147-A, nos seguintes termos: ‘‘Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade’’. A redação desse artigo possibilita sua aplicação tanto para perseguições físicas, como a virtuais. (Brasil, 1940, n.p.)

Essa modalidade de *stalking* ainda não recebeu muita atenção dos legisladores como um fenômeno social, considerando que a criminalização dessa conduta é algo muito recente. Isso demonstra a necessidade de uma investigação para apontar as possíveis lacunas que provavelmente poderão aparecer na aplicação dessa norma penal. (Silva, 2021, p. 44)

Entre as características dos *cyberstalking* está o envio de mensagens indesejadas, inapropriadas, que podem ser enviadas por uma pessoa conhecida ou desconhecida, com o intuito de se comunicar com a vítima, de forma contínua e persistente. Algumas fontes consideram a persistência como uma característica desse crime, especialmente quando as mensagens e tentativas de contato ultrapassam a décima vez, mesmo sem a vítima demonstrar interesse em continuar o diálogo. (Fornasier; Spinato; Ribeiro, 2022, p. 7)

A perseguição cibernética também ocorre constantemente em situações em que há ou houve um envolvimento amoroso entre o perseguidor e a vítima, seja essa relação interrompida ou extinta, ou até mesmo quando a relação apenas existiu na mente do perseguidor. Dessa forma, independentemente de ter havido ou não uma relação anterior entre a vítima e o autor, é provável identificar indícios de perseguição, o que pode acarretar em transtornos de ansiedade, depressão, dentre outros problemas psicológicos para a vítima. (Fornasier; Spinato; Ribeiro, 2022, p. 8)

Importante ressaltar que a perseguição obsessiva pode ocorrer, inicialmente, em relação a pessoas públicas e famosas. (Fornasier; Spinato, Ribeiro, 2022, p. 4) O perseguidor, que pode ser um anônimo ou que se identifica para a vítima, obcecado pela pessoa famosa, pode planejar atos, enviar mensagens anônimas, interagindo em publicações feitas pela vítima e até segui-lo pessoalmente, utilizando aplicativo *online* em que a celebridade compartilha sua localização.

A título de exemplo, temos o caso ocorrido no Brasil, em 2016, envolvendo a famosa modelo Ana Hickman:

[11] *Stalking* é o ato de perseguir e assediar alguém de forma persistente e indesejada, frequentemente ameaçando a integridade física, psicológica e a privacidade da vítima.

> A famosa modelo Ana Hickman e sua equipe foram atacadas por um homem, que perseguia a modelo nas redes sociais, e fazia várias postagens referentes à mesma, sendo completamente obcecado por tudo que a envolvia. Nesse caso o perseguidor era um homem que dizia amar a modelo, e claramente tinha uma relação fantasiosa com a mesma. Na oportunidade do ataque, munido de uma arma de fogo, investiu em um uma tentativa de ter um contato real, gerando um grave incidente em decorrência do qual o infrator perdeu sua vida. (Fornasier; Spinato, 2022, p. 5)

Assim, esse caso evidencia que o *cyberstalking* não deve ser considerado como mero aborrecimento no ambiente virtual. Embora muitos delitos comecem com interações nas comunidades *online*, eles podem evoluir para comportamentos violentos fora das telas, resultando em graves consequências, incluindo a morte de vítimas desse crime. (Fornasier; Spinato; Ribeiro, 2022, p. 5) A *internet* oferece um cenário atraente para os perseguidores cibernéticos e outros predadores *online*, pois o anonimato facilita a busca por vítimas, dificultando a identificação e responsabilização dos criminosos. (Silva, 2022, p. 22)

4. LEGISLAÇÃO PARA OS CRIMES CIBERNÉTICOS

O crescimento da *internet* e sua popularidade são evidentes, e hoje em dia, praticamente todos utilizam *smartphones*, *tablets* e computadores em suas rotinas. Contudo, a legislação ainda está em processo de adaptação para acompanhar as mudanças tecnológicas. Em um passado recente, os crimes passados no ambiente virtual eram tratados por analogia a tipos penais tradicionais, devido à ausência de tipificações específicas para as novas condutas criminais.

No Brasil, o tema de crimes virtuais é regulamentado por uma série de marcos legais que abordam diferentes aspectos relacionados aos crimes cibernéticos, à *internet*, à proteção de dados, dentre outros temas. Esses marcos incluem a convenção de Budapeste, a Lei n° 12.965/2014, conhecida como o marco civil da *internet*, Lei nº 12.737/2012 popularmente conhecida como Lei da Carolina Dieckmann, Lei n° 13.709/2018, a Lei geral de proteção de dados.

4.1 Convenção de Budapeste

Os crimes cibernéticos passaram a ser uma preocupação do Conselho da Europa na década de 1980, destacando-se com a adoção das orientações sobre os delitos envolvendo aparelhos tecnológicos e a tecnologia da informação nos processos criminais. A Convenção de Budapeste (Hungria, 2001), buscou harmonizar aspectos relativos ao Direito Penal substantivo dos países signatários, além de definir poderes e ações que facilitassem a persecução penal e estabelecer um regime ágil e eficaz de cooperação internacional, conforme evidencia o doutrinador Crespo. (Crespo, 2011, p. 31) Trata-se, de documentação de Direito Internacional Público, que foi elaborada pelo comitê de especialistas, no escopo de que os países signatários implementem normas de direito material que façam frente aos crimes cibernéticos. (Jesus, Milagre, 2016, p. 22)

Assim, a Convenção acerca dos crimes cibernéticos foi aberta na cidade de Budapeste na Hungria e firmada em 23 de novembro de 2001 por países da União Europeia. Além de contar com a adesão de nações como a Austrália, Japão e Estados Unidos. Este acordo internacional estabelece diretrizes para as políticas nacionais e propõe a harmonização das legislações, com a finalidade de combater de maneira eficaz os crimes cibernéticos. (Jesus; Milagre, 2016, p. 22)

A Convenção foi dividida em quatro capítulos: a) capítulo I, abarca as questões relacionadas às incriminações de certas condutas; b) Capítulo II, que trata do Direito Processual, determinando as condições gerais de salvaguardas relativas às provas; c) Capítulo III, aborda as ações relativas à cooperação internacional, incluindo questões sobre extradição; e d) Capítulo IV, contém as cláusulas finais da Convenção, comuns aos tratados internacionais. (Crespo, 2011, p. 31)

Destaca-se que decorridos mais de vinte anos desde sua entrada em vigor na ordem internacional, a Convenção de Budapeste permanece importante e atualizada, sendo ratificada por 68 Estados, membros e não membros do Conselho da Europa. O Brasil corroborou a Convenção em 2022 e a promulgou internamente com o Decreto 11.491/2023[12]. A inclusão do Brasil na Convenção de Budapeste era essencial, com a globalização e desenvolvimento da informática, houve uma amplificação da quantidade de usuários da *internet* e foram desenvolvidas novas formas de executar os crimes, intensificando a quantidade de vítimas e a dimensão do dano. (Murata; Torres, 2023, p. 1)

4.2 Lei n° 12.965/2014 – Marco civil da *internet*

A Lei nº 12.965/2014, conhecida como o marco civil da *internet*, foi criada pelo Ministério da Justiça com contribuições da sociedade civil e de especialistas, com origem no projeto de Lei nº 2.126/2011. Ela foi convertida em lei no dia 23 de abril de 2014, com o objetivo estabelecer um conjunto de direitos e deveres para os usuários da *internet*, buscando equilibrar a proteção legal com as práticas da cultura digital. (Cardozo, 2014, p. 25)

Essa lei surgiu para preencher uma lacuna normativa no sistema jurídico brasileiro, dando origem ao chamado marco civil da *internet*. Sua importância se destaca ao considerar que a inserção do Brasil na rede mundial de computadores ocorreu em 1995. Desde então, houve um processo contínuo de inclusão digital, que começou de forma lenta e restrita, mas acelerou nos últimos anos. (Leite; Lemos, 2014. p. 127)

É importante destacar que a liberdade de expressão deve ser considerada como princípio do uso da *internet* no Brasil, conforme o inciso I do artigo 3º da lei nº 12.965/2014. Esse princípio se fundamenta de maneira integrativa e sistemática com o princípio da cidadania, estabelecido no inciso I do art. 1ª da Constituição da República Federativa do Brasil de 1988. No aspecto inclusivo, o artigo 4º do marco civil da *internet* reforça o objetivo de garantir ‘‘o direito de acesso à *internet* a todos’’ em seu inciso I. (Leite; Lemos, 2014. p. 132)

O marco civil da *internet* foi elaborado com base em três princípios basilares que norteiam a relação das empresas que fornecem serviços de *internet* aos seus clientes, sendo eles: a neutralidade da rede, a proteção da privacidade e a liberdade de expressão. (Cardoso, 2014, p. 25) Contudo, além da liberdade de expressão, o direito à privacidade dos usuários de *internet* também tem sido objeto de violações por Estados e empresas. Assim como a liberdade de expressão, o direito à privacidade também é protegido pela Constituição. (Leite; Lemos, 2014, p. 74)

Além disso, o princípio da privacidade garante a inviolabilidade das comunicações dos usuários nas redes de computadores. Nesse sentido, a Lei nº 12.965/2014 impõe ao provedor de *internet* o dever de manter em sigilo as informações dos usuários. Quanto à fiscalização, a responsabilidade recai sobre a empresa provedora do serviço de *internet*, que é obrigada a manter

12

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.

os registros por um período mínimo de um ano. Caso as autoridades necessitem, elas podem exigir do provedor de *internet* os dados cadastrais que identifiquem os usuários, como nome completo, estado civil, endereço, entre outros. (Leite; Lemos, 2014, p. 156)

4.3 Lei n° 12.737/2012 – Lei da Carolina Dieckmann

Com o avanço da tecnologia, as conversas *online*, nas quais os interlocutores podem visualizar imagens e interagir em tempo real por meio de computadores ou *smartphones*, tornaram-se cada vez mais comuns no cotidiano global. Essas mudanças também levaram ao aumento do armazenamento de informações nesses dispositivos. No entanto, o ordenamento jurídico brasileiro não tinha uma lei específica para lidar com as violações das informações contidas nestes dispositivos. (Fuhr, 2022, p. 11)

O caso envolvendo a atriz Carolina Dieckmann, que teve seu computador invadido e seus arquivos pessoais roubados, resultando na exposição de suas fotos íntimas na *internet*, esse caso gerou comoção e indignação social. Em decorrência desse fato, foi editada e promulgada a Lei nº 12.737, em 30 de novembro de 2012, tipificando o crime de invasão de dispositivo informático. Ficando popularmente conhecida como a Lei da Carolina Dieckmann. (Fuhr, 2022, p. 11)

A Lei nº 12.737/2012, trata de crimes eletrônicos. Com sua aprovação, foi tipificado como crime o uso indevido de dados de cartões de crédito ou débito obtidos sem a autorização do legítimo titular. A lei penal equipara essa prática ao crime de falsificação de documento particular, punível com reclusão de um a cinco anos, além de multa. (Brasil, 1940, n.p.)

Outrossim, a mesma lei criminaliza a invasão de dispositivos eletrônicos alheios, como celulares, computadores, *tablets* ou caixas eletrônicos, que estejam conectados à *internet*. Essa prática, que envolve a obtenção ou adulteração de dados no sistema para conseguir uma vantagem ilícita, agora é considerada crime. (Fuhr, 2022, p. 14-15) A pena para esse tipo de infração é de três meses a um ano de prisão, além de aplicação de multa. Desse modo, com a promulgação dessa lei, invadir o dispositivo de alguém para buscar informações pessoais ou manipular dados financeiros pode resultar em graves consequências legais. (Brasil, 1940, n.p.)

O objetivo jurídico do crime é proteger a privacidade individual ou profissional armazenada em qualquer dispositivo informático, preservando o direito fundamental garantido no artigo 5º, inciso X, da Constituição Federal: ‘‘são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito de indenização pelo dano material ou moral decorrente de sua violação’’. (Fuhr, 2022, p. 11) Dessa forma, mesmo que uma informação seja postada em comunidades virtuais e acessível, isso não dá direito a terceiros de utilizar a foto ou informações em outro contexto sem prévia e expressa autorização para o uso da imagem.

A Lei da Carolina Dieckmann também prevê pena para o crime de invasão a quem produzir, oferecer ou vender programas de computadores que permitam a invasão, como, os *vírus* da *internet*, entre outros. Além disso, quem obtiver informações sigilosas ou violar comunicações eletrônicas privadas ou segredos comerciais, como senhas ou *e-mails*, está sujeito a uma pena maior, que varia de seis meses a dois anos de prisão. Essa pena pode ser aumentada de 1/3 a 2/3 se os dados obtidos forem divulgados ou comercializados, devido ao maior dano causado à vítima. (Pinheiro, 2021, p. 396)

Outra mudança trazida com a criação dessa lei, foi a criminalização da interrupção internacional do serviço de *internet* de utilidade pública, como a retirada do ar de sites públicos, geralmente cometida por *hackers*. A pena para esse crime foi estabelecida em um a três anos de detenção, além de aplicação de multa. Apesar de parecer uma medida adequada, a pena é

considerada bem baixa em comparação a outros países, onde esse tipo de conduta pode ser tipificado como crime de ciberterrorismo[13], com penas mais severas. Ademais, muitos novos tipos penais surgiram, mas não foram aprovados, pois estavam no Projeto de Lei Azevedo. (Pinheiro, 2021, p. 396)

Portanto, o crime de invasão do dispositivo informático se concretiza quando alguém invade o dispositivo informático de outra pessoa, violando mecanismos de segurança, com o objetivo de obter, adulterar ou destruir dados ou informações, ou de instalar vulnerabilidades no sistema. A Lei nº 12.737/2012 visa tipificar delitos informáticos, tratando das invasões a dispositivos tecnológicos, da interrupção ou perturbação telegráfica, telefônicos, desinformação em serviços de utilização pública, da falsificação de documentos e cartões. Além disso, essa lei tipifica condutas que, até então, eram tratadas como infrações penais. (Brasil, 1940, n.p.)

4.4 Lei n° 13.709/2018 – Lei Geral de Proteção de Dados

A ampliação do *cibercrime* ao decorrer dos anos gerou a necessidade de melhorar soluções efetivas e seguras para proteger os usuários contra possíveis ataques cibernéticos. Entre os métodos mais eficazes de garantir a segurança dos usuários e evitar quebras de dados, destaca-se a aplicação de leis específicas que definem critérios de segurança e oferecem diretrizes sobre o tratamento adequado dos dados. (Silva; Novais, 2023, p. 2)

A Lei nº 13.709/2018, conhecida como a lei geral de proteção de dados (LGPD), foi sancionada em 2018, mas entrou em vigor apenas em 2020. (Nunes, 2023, p. 17) A LGPD foi criada com o objeto de proteger direitos fundamentais como a privacidade, a intimidade, a honra, o direito à imagem e a dignidade. (Brasil, 1988, n.p.) Vale destacar que a necessidade de regulamentação e de leis específicas para a proteção de dados se intensificou com o rápido desenvolvimento e a disseminação da tecnologia no mundo, impulsionado pela globalização, que aumentou a importância do compartilhamento de informações. Isso significa que a tecnologia se tornou uma grande aliada e um recurso de alta relevância para os governantes e empresários. (Garrido, 2023, p. 105)

Destaca-se, também, que a LGPD, foi inserida no rol de direitos fundamentais do art. 5º da Constituição Federal de 1988, no seu inciso LXXIX, por meio da Emenda Constitucional nº 115, de 2022, *in verbis*: ‘‘é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais’’. (Brasil, 1988, n.p.) Outrossim, outro ponto abordado pela Lei nº 13.709/2018 é a exigência de consentimento dos dados, que deve ser fornecido de forma livre e expressa, autorizando o manejo dos seus dados para uma finalidade específica. A lei não admite autorizações genéricas, e o gerenciamento dos dados é vedado caso o consentimento tenha sido mediante vício de consentimento. (Brasil, 2018, n.p.)

A lei geral de proteção de dados representa uma inovação no Brasil e desempenha um papel crucial no crescimento econômico. Com a criação da lei, foi fomentada a confiança do consumidor, além de promover a economia digital e incentivar práticas de conformidade. A LGPD cria um ambiente adequado para o crescimento da economia sustentável, o aumento dos negócios e avanço tecnológico. (Garrido, 2023, p. 176)

---

[13] Ciberterrorismo é o uso de tecnologias da informação, como a *internet*, para realizar ataques cibernéticos com o objetivo de causar danos, pânico ou desestabilização em larga escala. Esses ataques podem incluir a interrupção de infraestruturas críticas, como redes de energia, sistemas financeiros, ou serviços de comunicação, e são realizados por grupos ou indivíduos com intenções terroristas. O ciberterrorismo visa causar medo, prejudicar governos, empresas ou a sociedade, e é uma ameaça crescente na era digital.

Além disso, ainda que a LGPD traga diretrizes sobre as sanções aplicáveis, o artigo 53 da lei determina que a Autoridade Nacional de Proteção de Dados (ANPD) será responsável por definir, por meio de regulamento próprio, as sanções administrativas para infrações à legislação, incluindo as sanções de multa. (Garrido, 2023, p. 46) A ANPD foi criada com o objetivo de proporcionar mais segurança e estabilidade para a aplicação da lei geral de proteção de dados. No Brasil, trata-se de um caso específico, pois muitos artigos da lei dependem de uma futura regulamentação pelos governantes. Portanto, caberá a eles realizarem as adequações necessárias para que a legislação tenha uma maior compatibilidade com a realidade social e econômica brasileira. (Garrido, 2023, p. 49)

5. OS DESAFIOS DA APLICAÇÃO DAS LEGISLAÇÕES ESTABELECIDAS PELO ORDENAMENTO JURÍDICO

É notório o aumento do desenvolvimento tecnológico na última década, que afetou a forma de comunicação e a perspectiva da sociedade. Nesse sentido, os crimes cibernéticos apresentam uma grave ameaça crescente e constante no cenário internacional atual. Com a evolução da tecnologia e a expansão da *internet*, a prática de crimes virtuais evoluiu de forma relevante, alterando o cenário da segurança cibernética e desafiando os recursos dos governos em todo o mundo de regular e controlar essas ações criminosas. (Maia; Costa, 2023, p. 3)

Atualmente, o ciberespaço está repleto de perigos, pois os *cybers* criminosos estão se tornando cada vez mais sofisticados e possuem conhecimento tecnológico para superar os sistemas que são considerados seguros. Ademais, esses criminosos desenvolvem técnicas para violar a segurança das redes e comprometer dados dos usuários, visando objetivos diversos, como roubo de informações pessoais, fotos, conversas e dados bancários.

Além disso, o Brasil até em 2012, reclamava por um dispositivo legal que tratasse de maneira abrangente os temas pertinentes aos crimes no ciberespaço. Podemos citar alguns países que desenvolveram leis referentes a crimes virtuais, como Portugal, com o advento da lei nº 109/1991; a França que alterou seu Código Penal Francês em 1988, pela Lei nº 88-19; e a Itália, que desde 1993 trata de alguma forma os delitos relacionados à informática. (Crespo, 2011, p. 31)

Por conseguinte, uma preocupação referente ao tema é a ausência de leis nacionais suficientes que abarque os crimes informáticos. Não distante, em 2012, foram aprovadas duas leis que representaram o pontapé para os crimes digitais: a Lei nº 12.735/2012[14] e a Lei nº 12.737/2012, que altera o Código Penal, tipificando os crimes virtuais e aumentando a punição para esses crimes. Desse modo, novas sanções para outros tipos de crimes digitais ocorreram, incluindo a invasão de computadores, a transmissão de *vírus* ou códigos que roubam cartões de crédito e débito sem autorização do titular do cartão. Já em 2014, foi promulgada a Lei nº 12.965, conhecida como o Marco Civil da *Internet*. (Lorenzo; Scaravelli, 2022, p. 7)

Um dos principais desafios no que tangue a natureza transnacional dos crimes digitais é que a *internet* transcende países. Isso permite que o cibercriminoso opere de qualquer local do mundo. O que exige das autoridades uma cooperação internacional sólida e eficaz para detectar, processar e prender os cibercriminosos. Contudo, em 2018 foi promulgada a Lei n° 13.709, que regulamentou a atividade cibernética. Essa lei foi um passo significativo para regulamentação dos crimes virtuais,

[14] Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

representando um esforço para alinhar as leis brasileiras com as leis internacionais de proteção de dados. (Almeida, 2023, n.p.)

A evolução do direito na era digital tem sido um esforço contínuo para se adaptar e evoluir. Com o surgimento da *internet* e suas tecnologias, novas questões jurídicas tornaram-se aparentes, exigindo uma reavaliação da legislação atualmente em vigor. De acordo com Silva e Novais (Silva; Novais, 2023, p. 3) os cibercrimes tornaram-se uma ameaça significativa em relação à segurança dos dados pessoais. Atualmente, existem diversos tipos de crimes virtuais, como a propagação indevida de dados, clonagem de cartões de crédito e roubo de identidade. O impacto dos crimes cibernéticos na sociedade é grave e pode causar grandes prejuízos.

A falta de conscientização da população sobre os riscos da utilização de aparelhos eletrônicos também é uma dificuldade. Os usuários da *web* muitas vezes não possuem compreensão das ameaças *online* e das práticas de segurança digital. Isso pode levar a comportamentos arriscados que facilitam a ocorrência de crimes cibernéticos. Essa lacuna deve ser sanada por esforço na educação pública para apoiar a conscientização sobre boas práticas e segurança *online* no mundo virtual. (Almeida, 2023, n.p.)

É importante, salientar que a conscientização acerca dos crimes cibernéticos deve ser propagada dentro das redes de ensino públicas, pois de acordo com dados do Ministério Público Federal (MPF) os maiores volumes de crimes se concentram nos crimes de pornografia infantil (501), apologia e incitação a crimes contra a vida (78) e o neonazismo (60), ocorrem também investigações de ocorrência de crimes de racismo, xenofobia, LGBTfobia e violação contra o direito das mulheres. (Ministério Público Federal, 2024, n.p.)

Além disso, de acordo com dados do Ministério dos Direitos Humanos e da Cidadania (MDHC) entre o período de 2017 a 2022, o tipo de crime de ódio mais denunciado na Central da *SaferNet* foi o crime de apologia a crimes contra a vida com 76,1 mil casos, seguido do crime de misoginia com 74,3 mil casos no total. Durante esse período, o crime de misoginia foi o crime de ódio que mais aumentou, superando a quantidade de 961 denúncias, em 2017, para 28,6 mil casos em 2022, refletindo um aumento de quase 30 vezes. Nos cinco anos também foram registradas 45,6 mil denúncias de racismo, 32,6 mil casos de neonazismo, 28,3 mil casos de LGBTfobia, 25,9 mil ocorrências de xenofobia e 10,2 mil incidentes de intolerância religiosa. (Gov.br, 2024, n.p.)

Outrossim, no Brasil não tem uma lei específica para a conduta criminosa de crime cibernético. A título de exemplo, pode-se analisar o caso em que o réu foi acusado de furto mediante fraude caracterizando um crime cibernético julgado pelo Tribunal de Justiça do Rio Grande do Sul, em 2015, (Apelação Criminal nº 70058702630)[15]. O julgamento evidencia a insuficiência de provas que comprovassem a autoria do crime, apesar da materialidade do delito reconhecida. (Rio Grande do Sul, 2015, n.p.)

---

[15] APELAÇÃO CRIMINAL. CRIME CONTRA O PATRIMÔNIO. FURTO MEDIANTE FRAUDE. CRIME CIBERNÉTICO. INSUFICIÊNCIA PROBATÓRIA.ABSOLVIÇÃO. Em que pese comprovação da materialidade do delito, a autoria restou duvidosa, uma vez que o conjunto probatório se mostrou insuficiente para demonstrá-la com a certeza necessária para embasar um juízo condenatório. Em se tratando de crime através do uso da internet, poderia o órgão ministerial diligenciar no sentido de identificar e rastrear o IP de conexão do agente e, a partir daí, identificar o usuário. Não basta que se identifique tão somente o titular da conta bancária destinaria. Ressalto que a inversão do ônus da prova não encontra lugar no processo penal. É do Ministério Público a obrigação de trazer subsídios comprobatórios da materialidade e da autoria do fato denunciado. No caso dos autos, a prova colhida após a instauração do contraditório não derruiu a dúvida que favorece ao acusado no processo penal. Não sendo possível a condenação com base apenas em indícios e suposições, impõe-se a absolvição do acusado, com fundamento no art. 386, VII, do CPP. APELAÇÃO PROVIDA.

Dessa forma, conforme o julgado mencionado, observa-se que a legislação ainda possui lacunas em casos de crimes cibernéticos, absolvendo a maioria dos criminosos, ocasionando no aumento do índice de crimes virtuais impunes. (Trindade; Albino; Stegmann, 2022, n.p.) Portanto, as dificuldades contemporâneas acerca da regulamentação dos crimes cibernéticos são um reflexo da rápida evolução da tecnologia e das complexidades relacionadas ao espaço virtual.

A regulamentação eficaz desses crimes requer uma análise completa que considere a natureza global da conduta ilícita, a contínua inovação dos métodos dos criminosos, a conscientização da população, a privacidade e o alinhamento das legislações internacionais. Assim, para abordar os desafios exigem uma colaboração entre governos, setor privado, entidades civis para proteger e garantir um espaço digital mais seguro e regulado. (Almeida, 2023, n.p.)

6. CONCLUSÃO

A *internet* apresentou diversos avanços e benefícios para a sociedade, desde a democratização do acesso à *internet* até facilidade de comunicação entre pessoas em diferentes partes do mundo. Contudo, conforme abordado ao longo desse artigo, surgiram também diversos desafios, especialmente no que tange acerca da segurança, privacidade e ética no ciberespaço. A *internet*, em sua imensidão, transformou-se em um espaço onde a liberdade de expressão é celebrada, mas também onde os crimes de ódio entraram em um espaço favorável para se expandir.

Os crimes cibernéticos evoluíram de apenas curiosidades do funcionamento dos computadores para ameaças globais. A regulamentação progrediu para tratar essas ameaças, mas a dificuldade ainda permanece. As entidades governamentais executam um papel essencial na prevenção e segurança contra os cibercrimes, demandando investimentos em inovações tecnológicas, conscientização para os indivíduos e cooperação internacional. A contínua modificação às mudanças tecnológicas é primordial para combater a ameaça à segurança cibernética.

Além disso, os crimes cometidos via *internet* estão presentes em todo globo, contudo, o Brasil encontra-se atrasado em comparação a outros países por não regulamentar uma legislação própria e adequada para penalizar os criminosos que infringem as condutas criminosas. A ausência de tipificação adequada para condutas ofensivas praticadas no mundo virtual, causando grande insegurança jurídica e social no âmbito jurídico brasileiro.

A evolução histórica dos crimes cibernéticos revela que eles tiveram origem em atos de entusiastas digitais, mas de forma rápida se tornaram em uma forma de crime sofisticado e lucrativo. Atualmente, os grupos de *hackers* e organizações criminosas estão envolvidos em atividades cibernéticas ilegais que têm implicação para a segurança coletiva.

Acerca das legislações, foi analisada a Convenção de Budapeste (Hungria, 2001) que buscou harmonizar aspectos relativos ao Direito Penal substantivo dos países signatários, além de definir poderes e ações que facilitassem a persecução penal e estabelecer um regime ágil e eficaz de cooperação internacional. A Lei nº 12.965/2014, conhecida como o Marco Civil da Internet, trouxe mudanças para que as empresas que atuam no comércio eletrônico tenham a obrigação de fornecer informações claras sobre seus produtos, fornecedores e serviços. Além disso, a Lei nº 12.737/2012, conhecida como Lei da Carolina Dieckmann e a Lei nº 13.709/2018 (LGPD).

Ademais, nesse artigo ressaltou-se os desafios da aplicação das legislações estabelecidas pelo ordenamento jurídico, em que foi mencionado sobre os desafios no que tangue a natureza transnacional dos crimes digitais é que a *internet* transcende países. Isso permite que o

cibercriminoso opere de qualquer local do mundo. O que exige das autoridades uma cooperação internacional sólida e eficaz para detectar, processar e prender os cibercriminosos.

A dificuldade do crescimento dos crimes cibernéticos na sociedade digital contemporânea, o progresso da tecnologia oferece diversas oportunidades, contudo, também apresenta desafios significativos, desde a invasão de sistemas, estelionatos virtuais, assédio *online*, dentre outros. Dessa forma, consta que o contexto de crimes cibernéticos está em constante evolução, conforme os *cybers* criminosos são habilidosos e a cada vez evoluindo seus métodos criminosos.

Analisados os pontos citados no artigo fica claro que a tecnologia continua a evoluir. Dessa forma, é necessário que a sociedade, governos e empresas adotem medidas para proteger sistemas e informações críticas, bem como para desenvolver estratégias que possam identificar e responsabilizar os autores de crimes cibernéticos.

Por fim, é necessário a prevenção e a proteção contra esses delitos requerem uma abordagem multidisciplinar, que envolve segurança cibernética, legislação atualizada e a cooperação internacional focada no treinamento e capacitação de agentes focados em combater esses crimes, para enfrentar ameaças transnacionais.

REFERÊNCIAS

ALMEIDA, Daiana. **A eficácia da aplicação da legislação de crimes cibernéticos no combate a pedofilia digital**. Revista ft. Rio de Janeiro/RJ. v. 27. n. 127. n.p.Disponível em: A EFICÁCIA DA APLICAÇÃO DA LEGISLAÇÃO DE CRIMES CIBERNÉTICOS NO COMBATE A PEDOFILIA DIGITAL – ISSN 1678-0817 Qualis B2 (revistaft.com.br). Acesso em: 25 ago. 2024.

ALMEIDA, Ruanh Neres de. **Estelionato virtual no direito brasileiro.** 2023.Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/6205 Acesso em: 17 out. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, Presidência da República, 5 de out. de 1988. Disponível em: Constituição (planalto.gov.br). Acesso em: 13 ago. 2024.

BRASIL. **Decreto lei n° 2.848, de 7 de dez. de 1940**. Código Penal. Rio de Janeiro, 7 de dez. de 1940. Disponível em: DEL2848 (planalto.gov.br). Acesso em: 05 jun. 2024.

BRASIL. **Decreto n° 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 nov. de 2001. Brasília, 12 de abril de 2023. Disponível em: D11491 (planalto.gov.br). Acesso em: 11 jun. 2024.

BRASIL. **Lei nº 12.735, de 30 de Novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, 30 de nov. de 2012. Disponível em: https://www.planalto.gov.br/ccivil03/ato2011-2014/2012/lei/l12735.htm. Acesso em: 11 jun. 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. Brasília, 30 nov. 2012.
Disponível em: https://www.planalto.gov.br/ccivil03/ato2011-2014/2012/lei/l12737.htm. Acesso em: 4 jun. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 23 de abr. de 2014. Disponível em: L12965 (planalto.gov.br). Acesso em: 16 ago. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 14 ago. de 2018. Disponível em: L13709 (planalto.gov.br). Acesso em: 16 ago. 2024.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília, 27 de mai. de 2021.
Disponível em: L14155 (planalto.gov.br) . Acesso em: 05 jun. 2024.

CAVALCANTI NETO, Gabriel de Oliveira. **Direito penal cibernético: da evolução legislativa à necessidade de tipificação de crimes cibernéticos próprios.** Revista Foco. *Online*. v. 16 n. 6.n.p. Disponível em: https://doi.org/10.54751/revistafoco.v16n6-028. Acesso em: 11 jun. 2024.

CAPEZ, Fernando. **Curso de direito penal: parte especial: arts. 121 a 212. v.2**. Rio de Janeiro: https://integrada.minhabiblioteca.com.br/#/books/9788553622672/Grupo GEN, 2024. *E-book*. ISBN 9788553622672. Disponível em: . Acesso em: 08 set. 2024.

CRESPO, Marcelo Xavier de F. **Crimes digitais.** [Digite o Local da Editora]: SRV Editora LTDA, 2011. E-book. ISBN 9788502136663. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502136663/. Acesso em: 05 jun. 2024.

CUNHA, Vinícius Ferreira da; CORTIZO , Vitor Martins. **Crimes cibernéticos: implicações legais, eficácia das leis existentes e necessidade de adaptação do sistema legal a era digital.** Revista Acadêmica Online , *[S. l.]*, v. 10, n. 51, p. 1–18, 2024. Disponível em: https://www.revistaacademicaonline.com/index.php/rao/article/view/122. Acesso em: 25 ago. 2024.

DE CASTRO, B. P.; NAZARETH, L.; MARQUES, L.; FERREIRA, N. **Crimes contra a honra: Uma análise da ineficácia das leis existentes frente aos delitos cometidos nas redes sociais**. Eletrônico Faculdades Integradas Vianna Júnior, [S. l.], v. 13, n. 1, p. 19, 2021. Disponível em: https://www.jornaleletronicofivj.com.br/jefvj/article/view/805. Acesso em: 17 out. 2024.

DE OLIVEIRA FORNASIER, Mateus; SPINATO, Tiago Protti; RIBEIRO, Fernanda Lencina.

Cyberstalking: perseguição, privacidade e suas consequências no ambiente de rede. Revista do Mestrado em Direito da UCB, p. 1-28, 2022. Disponível em: https://portalrevistas.ucb.br/index.php/rvmd/article/view/12116. Acesso em: 14 ago. 2024.

Federal Bureau of Investigation (FBI). **Relatório de Crimes na Internet 2019 Lançado.** Disponível em: Relatório de Crimes na Internet de 2019 Divulgado — FBI. Acesso em: 11 jun. 2024.

FERREIRA, Luana Noemia dos Santos. **Stalking e violência de gênero: a criminalização do stalking com medida protetiva ao feminicídio.** 2024. Trabalho de Conclusão de Curso. Universidade Federal do Rio Grande do Norte. Disponível em: https://repositorio.ufrn.br/handle/123456789/59908. Acesso em: 16 out. 2024.

FÜHR, Isis. **Crimes cibernéticos: uma análise sobre condutas criminosas no ambiente virtual e o tratamento conferido pelo ordenamento jurídico brasileiro.** Revista Científica Semana Acadêmica, Fortaleza, ano MMXXII, n. 000227, 18 nov. 2022. Disponível: https://semanaacademica.org.br/artigo/crimes-ciberneticos-uma-analise-sobre-condutas-criminosas-no-ambiente-virtual-e-o-tratamento. Acesso em: 15 ago. 2024.

GABRIEL MACHADO, D. R.; GROTT, S. **Estelionato virtual.** Revista Científica Multidisciplinar do CEAP, v. 4, n. 1, p. 10, 9 jun. 2022. Disponível em: http://periodicos.ceap.br/index.php/rcmc/article/view/149. Acesso em 14 ago. 2024.

GARRIDO, Patricia P. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD)**. Rio de Janeiro: Grupo GEN, 2023. *E-book.* ISBN 9786555599480. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555599480/. Acesso em: 16 ago. 2024.

GARUTTI, Hallifer Augusto; DE BRITO, Alexis Couto. **Crimes cibernéticos: uma análise sobre o estelionato virtual.** Revista PGM-Procuradoria Geral do Município de Fortaleza, v. 31, n. 1, 2023. Disponível em: Crimes cibernéticos: uma análise sobre o estelionato virtual | Revista PGM - Procuradoria Geral do Município de Fortaleza. Acesso em: 24 out. 2024.

GRECO, Rogério. **Curso de Direito Penal: artigos 213 a 361 do código penal. v.3**. [Digite o Local da Editora]: Grupo GEN, 2023. E-book. ISBN 9786559774319. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559774319/. Acesso em: 19 mai. 2024.

HENRIQUES, Thiago Alves; GONÇALVES, Samuel Martins. **Crimes digitais: Análise sobre estelionato virtual.** Revista Eletrônica de Ciências Jurídicas, [S. l.], v. 14, n. 1, 2024. Disponível em: https://revista.fadipa.br/index.php/cjuridicas/article/view/567 . Acesso em: 14 ago. 2024.

INTERNATIONAL IT. **Anuário de Segurança Pública 2023: crimes digitais aumentam 65,2%**. Disponível em: https://www.internationalit.com/post/anu%C3%A1rio-de-seguran%C3%A7a-p%C3%BAblica-2023-crimes-digitais-aumentam-65-2. Acesso em: 24 out. 2024.

JÊIOR, Júlio César ALEXANDRE. **Cibercrime: um estudo acerca do conceito de crimes informáticos.** Revista Eletrônica da Faculdade de Direito de Franca, v. 14, n. 1, p. 341-351, 2019. Disponível em: https://doi.org/10.21207/1983.4225.602. Acesso em: 08 out. 2024.

JESUS, Damásio de; MILAGRE, José A. **Manual de crimes informáticos** . [Digite o Local da Editora]: SRV Editora LTDA, 2016. *E-book.* ISBN 9788502627246. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502627246/ . Acesso em: 15 jun. 2024.

LEITE, George S.; LEMOS, Ronaldo. **Marco Civil da Internet**. Rio de Janeiro: Grupo GEN, 2014. *E-book.* ISBN 9788522493401. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522493401/ . Acesso em: 15 ago. 2024.

LORENZO, Larissa Papandreus; SCARAVELLI, Gabriela Piva. **5 Cibercrime e a legislação brasileira.** LORENZO, Larissa Papandreus. SCARAVELLI, Gabriela Piva. Diálogos e Interfaces do Direito-FAG, v. 4, n. 1, p. 104-122, 2021. Disponível em: 5 CIBERCRIMES E A LEGISLAÇÃO BRASILEIRA | Diálogos e Interfaces do Direito - FAG. Acesso em: 11 set. 2024.

LUMI KAMIMURA MURATA, D. A. M.; RITZMANN TORRES, M. P. **A convenção de budapeste sobre os crimes cibernéticos foi promulgada, e agora?**. Boletim IBCCRIM, [S. l.], v. 31, n. 368, 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575. Acesso em: 24 out. 2024.

MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. **Crimes cibernéticos**. Revista Ibero-americana de Humanidades, Ciências e Educação, *[S. l.]*, v. 9, n. 10, p. 109–126**,** 2023. DOI: 10.51891/easy.v9i10.11580. Disponível em: CRIMES CIBERNÉTICOS | Revista Ibero-Americana de Humanidades, Ciências e Educação (periodicorease.pro.br). Acesso em: 2 jun. 2024.

MINISTÉRIO DOS DIREITOS HUMANOS E DA CIDADANIA. Incitação à violência contra a vida na internet lidera violações de direitos humanos, com mais de 76 mil casos em cinco anos, aponta ObservaDH. Portal Gov.br, 2024. Disponível em: Incitação à violência contra a vida na internet lidera violações de direitos humanos com mais de 76 mil casos em cinco anos, aponta ObservaDH — Ministério dos Direitos Humanos e da Cidadania Acesso em: 24 out. 2024.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Convenção de Budapeste é promulgada no Brasil. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: 24 out. 2024.

MINISTÉRIO PÚBLICO FEDERAL. 2024. MPF destaca números da atuação na prevenção e combate a crimes cibernéticos no Dia da Internet Segura 2024. **Disponível:** MPF destaca números da atuação na prevenção e combate a crimes cibernéticos no Dia da Internet Segura 2024 — Procuradoria-Geral da República. Acesso em: 25 ago. 2024.

MORAES, Alexandre de. **Direito Constitucional**. **39th ed. Rio de Janeiro: Atlas, 2023. *E-book***. p.76. ISBN 9786559774944. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559774944/. Acesso em: 08 out. 2024.

NUCCI, Guilherme de S. **Curso de Direito Penal: Parte Geral: arts. 1º a 120. v.1.** [Digite o Local da Editora]: Grupo GEN, 2023. E-book. ISBN 9786559646852. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559646852/. Acesso em: 11 jun. 2024.

NUNES, Deborah Batista. **Crimes cibernéticos e a legislação penal brasileira**. 2023. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/6562. Acesso em: 13 ago. 2024.

Ordem de Advogados do Brasil Nacional (OAB). **Artigo: O jogo mortal e criminoso: Baleia Azul.** Disponível em: https://www.oab.org.br/noticia/54991/artigo-o-jogo-mortal-e-criminoso-baleia-azul. Acesso em: 12 jun. 2024

OTSU, Denise Pereira. **Crimes cibernéticos e os limites da liberdade de expressão nas redes.** Repositório Universitário da Ânima (RUNA), São Paulo, 2023. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/35166/1/CRIMES%20CIBERNE%CC%81TICOS%20%281%29.pdf. Acesso em: 11 jun. 2024.

PINHEIRO, Patrícia P. **Direito Digital**. [Digite o Local da Editora]: SRV Editora LTDA, 2021. *E-book.* ISBN 9786555598438. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 09 jun. 2024.

REIS, Ariovaldo Nascimento Ribeiro; VIANA, Geraldo Denison**. Crimes virtuais: legislações insuficientes ou ineficiência das autoridades competentes?.** Revista Ibero-Americana de Humanidades, Ciências e Educação, [S. l.], v. 7, n. 10, p. 1607–1626, 2021. DOI: 10.51891/rease.v7i10.2684. Disponível em: https://periodicorease.pro.br/rease/article/view/2684. Acesso em: 24 out. 2024.

SILVA, Dickson Carvalho Gonçalves da**. Crimes cibernéticos: limites e desafios na investigação.** 2022. Disponível em: http://repositorio.undb.edu.br/jspui/handle/areas/834. Acesso em: 13 ago. 2024.

SILVA, Larissa Martins da. **Tipificação do stalking: uma análise sobre a perseguição enquanto crime no Brasil.** 2021. Disponível em: http://repositorio.ufc.br/handle/riufc/69082. Acesso em: 16 out. 2024.

SILVA, Ronaldo Couto da; NOVAIS, Thyara Gonçalves. **A lei geral de proteção de dados e sua aplicação no combate aos crimes cibernéticos: desafios e perspectivas.** Revista Ibero-Americana de Humanidades, Ciências e Educação, [S. l.], v. 9, n. 10, p. 4679–4703, 2023. DOI: 10.51891/rease.v9i10.12254. Disponível em: https://periodicorease.pro.br/rease/article/view/12254. Acesso em: 17 out. 2024.

SOUZA, Kadmiel Duarte de. **Lei geral de proteção de dados (LGPD): impactos, desafios e perspectivas no cenário jurídico e empresarial no Brasil.** 2024. Disponível em: http://104.207.146.252:8080/xmlui/handle/123456789/771. Acesso em: 16 ago. 2024.

TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico**. [Digite o Local da Editora]: SRV Editora LTDA, 2024. *E-book.* ISBN 9788553622344. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553622344/. Acesso em: 11 jun. 2024.

Rio Grande do Sul, Tribunal de Justiça do Estado do Rio Grande do Sul. Apelação em crime contra o patrimônio (Furto/ Roubo). **Apelação Criminal nº 70058702630**. 7ª Câmara Criminal.Apelante: Gustavo Moraes Kubiaki. Apelado: Ministério Público. Relator Desembargador: Carlos Alberto Etcheverry. Rio Grande do Sul, 20 de agosto de 2015. Acesso em: 25 ago. 2024.

RODRIGUES, GIAN CARLOS GONÇALVES SANDRA. **Crimes cibernéticos.** Disponível em: TCC Completo - ABNT Padrão institucional. Acesso em: 18 out. 2024.

TORMEN, Chalidan Adonai Callehgari. **Crimes cibernéticos: (im) possibilidades de coerção.** ‘‘URI Campus de Erechim Departamento de Ciências Sociais Aplicadas Curso de Direito.’’ 2018. Disponível em: CRIMES CIBERNÉTICOS. Acesso em: 18 out. 2024.

TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO. **Operação da Justiça: mais de 6,2 mil sentenças e decisões proferidas em ações sobre violência doméstica**. TJRJ, 2024. Disponível em: https://www.tjrj.jus.br/web/portal-conhecimento/noticias/noticia/-/visualizar-conteudo/5736540/6447772. Acesso em: 24 out. 2024.

TRINDADE, Hairton. ALBINO, Matheus. STEGMANN, Vinícius. **Crimes cibernéticos: a fragilidade no ordenamento jurídico.** Revista ft. 2022. Disponível em: CRIMES CIBERNÉTICOS: A FRAGILIDADE NO ORDENAMENTO JURÍDICO BRASILEIRO – ISSN 1678-0817 Qualis B2 (revistaft.com.br). Acesso em: 25 ago. 2024.

AGRADECIMENTOS

Gostaria de agradecer a Deus, que me deu forças para chegar até aqui. Agradeço aos meus pais, que acreditaram na minha capacidade, e ao meu noivo Henrique, cujo apoio incondicional foi essencial durante minha jornada acadêmica. Sou grata à Professora Me. Caroline Lima Ferraz pelas orientações e correções deste artigo. Por fim, agradeço ao meu orientador Me. João de Deus, que ouviu minhas ideias, me orientou e me ajudou na construção deste artigo. Todas essas pessoas foram fundamentais para a conclusão deste artigo.