



CENTRO DE ESTUDO SUPERIOR DE ITAITUBA – LTDA  
FACULDADE DE ITAITUBA - FAI  
CURSO DE BACHARELADO EM DIREITO

FABIANNE COSTA FERREIRA

## **CRIMES CIBERNÉTICOS E A EFICÁCIA DAS LEIS PENAIS BRASILEIRAS**

Itaituba-PA  
2025

FABIANNE COSTA FERREIRA

## **CRIMES CIBERNÉTICOS E A EFICÁCIA DAS LEIS PENAIS BRASILEIRAS**

Trabalho de Conclusão de curso apresentado à  
Faculdade de Itaituba para obtenção de Título em  
Bacharel em Direito.

Orientador: Profº. Esp. Alexandre do Rosario Brito.

Itaituba-PA  
2025

FERREIRA, Fabianne Costa.

**CRIMES CIBERNÉTICOS E A EFICÁCIA DAS LEI PENAS BRASILEIRAS** / Fabianne Costa Ferreira. Itaituba: FAI, 2025.

45 f.: il.

Orientador: Profº. Esp. Alexandre do Rosário Brito

Trabalho de Conclusão de Curso (Graduação) - Faculdade de Itaituba, 2025.

1. Cibersegurança. 2. Crimes cibernéticos. I. BRITO, Alexandre do Rosário. II. Faculdade de Itaituba. Itaituba, BR – PA, 2025.

FABIANNE COSTA FERREIRA

**CRIMES CIBERNÉTICOS E A EFICÁCIA DAS LEIS PENAIS BRASILEIRAS**

Trabalho de Conclusão de curso apresentado à  
Faculdade de Itaituba para obtenção de Título em  
Bacharel em Direito.

Orientador: Prof. Alexandre do Rosário Brito

BANCA EXAMINADORA:

Presidente: \_\_\_\_\_ Nota: \_\_\_\_\_

Prof.(a)

Orientador: \_\_\_\_\_ Nota: \_\_\_\_\_

Prof.(a)

Avaliador(a): \_\_\_\_\_ Nota: \_\_\_\_\_

Prof.(a)

Resultado: \_\_\_\_\_ Média: \_\_\_\_\_

Itaituba-PA, \_\_\_\_\_ de \_\_\_\_\_ de 2025

“Dedico este trabalho primeiramente ao nosso Senhor Deus, por permitir que a cada dia eu tivesse forças para lutar e poder concluir esta jornada, ao meu esposo, minha família, amigos, docentes e ao meu orientador que foram cruciais nesta jornada acadêmica”.

## **AGRADECIMENTO**

Agradeço primeiramente a Deus, por me guiar e fortalecer.

À memória da minha mãe, que sempre será minha maior fonte de inspiração e motivação. Sua lembrança me impulsionou a seguir em frente.

Ao meu pai, pelo apoio e incentivo que serviram de alicerce para as minhas realizações.

Ao meu esposo, David Willy, que esteve ao meu lado em todos os momentos

À minha irmã Fábiana que sempre esteve presente nos momentos mais difíceis dessa trajetória.

Ao meu orientador, Alexandre do Rosário Brito, pela orientação e paciência ao longo deste trabalho.

Aos amigos e colegas, pelo suporte e companheirismo.

À FAI e aos professores, por todo o conhecimento e suporte.

E a todos que, de alguma forma, contribuíram para a realização deste TCC, meu sincero obrigada.

*"Porque sou eu que conheço os planos que tenho para vocês", diz o Senhor, 'planos de fazê-los prosperar e não de causar dano, planos de dar a vocês esperança e um futuro'".*

*Jeremias 29:11*

## **RESUMO**

A medida que a tecnologia e os desenvolvimentos computacionais continuam, os crimes digitais estão surgindo e se desenvolvendo paralelamente. As empresas estão desenvolvendo, endossando e implementando soluções e tecnologias para lidar com esses riscos. No entanto, o risco continua a crescer devido a várias atividades entre os usuários de tecnologia. Como as informações se tornaram um ativo essencial para as organizações, há uma necessidade cada vez maior de explorar vários métodos, estratégias e tecnologias para proteger essas informações. O objetivo é garantir e manter a confidencialidade, a integridade e a disponibilidade como prioridades fundamentais. Quais são os crimes cibernéticos predominantes? Como o sistema jurídico brasileiro trata esses delitos? O objetivo principal é demonstrar o nível inadequado de preparo dos usuários na utilização de meios eletrônicos. Além disso, busca-se destacar o atraso significativo do Brasil na formulação de uma estratégia eficaz para combater o crime cibernético. A discussão se concentrará na escassez de pessoal qualificado para conduzir investigações e analisar ataques cibernéticos, bem como na ausência de uma legislação abrangente para lidar com várias formas de ameaças cibernéticas.

**Palavras- chave:** Cibersegurança. Sociedade. Crimes cibernéticos.

## **ABSTRACT**

As technology and computing developments continue, digital crimes are emerging and developing in parallel. Companies are developing, endorsing and implementing solutions and technologies to deal with these risks. However, the risk continues to grow due to various activities among technology users. As information has become an essential asset for organizations, there is an increasing need to explore various methods, strategies and technologies to protect this information. The aim is to guarantee and maintain confidentiality, integrity and availability as key priorities. What are the most prevalent cybercrimes? How does the Brazilian legal system deal with these crimes? The main objective is to demonstrate the inadequate level of preparation of users in the use of electronic media. In addition, it seeks to highlight Brazil's significant delay in formulating an effective strategy to combat cybercrime. The discussion will focus on the shortage of qualified personnel to conduct investigations and analyze cyber-attacks, as well as the absence of comprehensive legislation to deal with various forms of cyber threats.

**Keywords:** Cybersecurity. Society. Cybercrime.

## SUMÁRIO

|                                                                      |           |
|----------------------------------------------------------------------|-----------|
| <b>1 INTRODUÇÃO .....</b>                                            | <b>11</b> |
| <b>2 FUNDAMENTAÇÃO TEÓRICA.....</b>                                  | <b>13</b> |
| 2.1 SURGIMENTO DOS CRIMES CIBERNÉTICOS.....                          | 13        |
| <b>2.1.1 Conceito de Crimes Cibernéticos.....</b>                    | <b>13</b> |
| 2.2 CRIMES CIBERNÉTICOS EM ESPÉCIE.....                              | 15        |
| <b>2.2.1 Ameaça.....</b>                                             | <b>15</b> |
| <b>2.2.2 Racismo (e outras formas de preconceito).....</b>           | <b>16</b> |
| <b>2.2.3 Pornografia Infantil.....</b>                               | <b>17</b> |
| <b>2.2.4 Estelionato.....</b>                                        | <b>19</b> |
| <b>2.2.5 O cyberbullying.....</b>                                    | <b>20</b> |
| <b>3 LEGISLAÇÃO BRASILEIRA.....</b>                                  | <b>25</b> |
| 3.1 LEI DO MARCO CIVIL DA INTERNET.....                              | 26        |
| 3.2 A INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS.....                      | 27        |
| 3.3 QUESTÕES JURISPRUDENCIAIS.....                                   | 30        |
| <b>3.3.1 Caso Marielle Franco (Geofecing).....</b>                   | <b>30</b> |
| <b>3.3.2 Importância da Cadeia de Custódia da prova Digital.....</b> | <b>32</b> |
| <b>3.3.3 Leis e Regulamentos Relevantes no Brasil.....</b>           | <b>32</b> |
| <b>3.3.4 Análise das Implicações Jurídicas e Práticas.....</b>       | <b>34</b> |
| <b>4 METODOLOGIA .....</b>                                           | <b>36</b> |
| 4.1 MÉTODOS E INSTRUMENTOS.....                                      | 36        |
| 4.2 COLETA DOS ESTUDOS .....                                         | 36        |
| 4.3 CRITÉRIOS DE INCLUSÃO E EXCLUSÃO: REVISÃO BIBLIOGRÁFICA.....     | 36        |
| 4.4 ANÁLISE DOS ESTUDOS .....                                        | 37        |
| 4.5 ASPECTOS ÉTICOS DA PESQUISA .....                                | 37        |
| <b>5 RESULTADOS E DISCUSSÃO.....</b>                                 | <b>38</b> |
| 5.1 ACHADOS DA PESQUISA .....                                        | 38        |
| <b>6 CONSIDERAÇÕES FINAIS.....</b>                                   | <b>41</b> |
| <b>REFERÊNCIAS.....</b>                                              | <b>43</b> |

## 1 INTRODUÇÃO

Na era da digitalização, a maioria dos indivíduos das nações industrializadas dedica uma parte significativa de sua existência ao reino intangível conhecido como Internet. Nossa identidade digital abrange vários aspectos, como redes sociais, pesquisas na Internet, publicações em blogs e outras formas de conteúdo on-line. Ela não se limita apenas aos dados, mas também inclui as informações contidas em nossas palavras, fotos e imagens que decidimos compartilhar. Além disso, com o passar do tempo, realizamos um número cada vez maior de tarefas na Internet, desde compras de rotina até transações financeiras.

Portanto, a Internet serve como uma plataforma de longa data onde vários crimes são cometidos diariamente, com consequências prejudiciais para milhões de pessoas em todo o mundo. Quais são os crimes cibernéticos predominantes? Como a legislação brasileira aborda esses crimes? O objetivo principal é demonstrar o nível inadequado de preparo dos usuários na utilização dos meios eletrônicos. Além disso, pretende-se destacar o atraso significativo do país na formulação de uma estratégia eficaz de combate ao crime cibernético. Além disso, busca discutir a escassez de pessoal qualificado para conduzir investigações e analisar a ausência de legislação para tratar de várias formas de ataques cibernéticos.

Este estudo se concentra nas origens e na definição do crime cibernético. Além disso, ele enfatiza a utilização da Internet como um meio anônimo para a prática de atividades criminosas, com o objetivo de detectar e impedir esses atos fraudulentos. Um problema que surge é o rápido crescimento desses crimes e a incapacidade de acompanhar o ritmo das leis nacionais. A velocidade com que esses crimes estão evoluindo é impressionante, o que torna desafiadora a promulgação de uma legislação que os trate com eficácia.

Também examinaremos a legislação nacional atual e seus esforços para combater os criminosos responsáveis por esses crimes. Este estudo tem como objetivo examinar a legislação brasileira referente ao crime cibernético e explorar possíveis estratégias para o desenvolvimento de estruturas legais em resposta às atividades criminosas cibernéticas.

A abordagem empregada para atingir os objetivos declarados neste estudo inclui a realização de uma extensa revisão da literatura relevante em um curto espaço de tempo. Foram encontrados vários artigos on-line relacionados ao tópico. A partir

disso, pode-se inferir que a metodologia utilizada foi a pesquisa bibliográfica e sua abordagem explicativa (GERHARDT & SILVEIRA, 2009). A coleta de dados foi feita em diversos meios, incluindo livros físicos e eletrônicos, artigos, periódicos e revistas.

Este estudo emprega metodologias de pesquisa bibliográfica, utilizando as fontes primárias e secundárias indicadas anteriormente. Em termos de sua intenção, pode ser classificado como explicativo, pois busca elucidar uma determinada ocorrência. Os resultados obtidos são quantitativos e a abordagem utilizada baseia-se principalmente em evidências documentais (ALVES, 2013).

## **2 FUNDAMENTAÇÃO TEÓRICA**

### **2.1 SURGIMENTO DOS CRIMES CIBERNÉTICOS**

O advento de novas tecnologias acelerou o aumento dos crimes cibernéticos, que podem ser cometidos por meio de dispositivos técnicos, com um número significativo de crimes sendo executados pela Internet. A Internet permite o anonimato, o que, por sua vez, promove uma sensação de impunidade entre os indivíduos, facilitando, assim, a prática de crimes virtuais por usuários com menos conhecimento de informática. Consequentemente, os confrontos que antes ocorriam apenas na esfera física agora se deslocaram para a esfera virtual, conforme afirma Nascimento (2010).

O grande número de usuários e o rápido influxo de informações resultaram em efeitos e ameaças globais cada vez maiores. Atualmente, um número significativo de pessoas dedica mais tempo ao envolvimento com a Internet do que com a realidade física. O advento da *World Wide Web* facilitou a solução remota de problemas e as conexões interpessoais. Entretanto, também resultou em maior vulnerabilidade das informações pessoais e exigiu o desenvolvimento de legislação para combater a proliferação de crimes cibernéticos diários.

Essas atividades ilegais surgiram após um aumento substancial na população de usuários da Internet, na qual existem vários indivíduos que exploram essa recente inovação (DIAS, 2021).

#### **2.1.1 Conceito de Crimes Cibernéticos**

Embora possa haver diferenças na doutrina sobre a conceituação de crimes cometidos por meios eletrônicos, um número significativo de especialistas os classifica como crimes cibernéticos. Sérgio Marcos Roque define crime cibernético como qualquer comportamento legalmente considerado crime que envolva o uso de um computador como ferramenta ou como alvo do crime (ROQUE, 2007, p. 26).

Vários crimes são comportamentos ilícitos praticados por indivíduos que empregam vários métodos para perpetrar golpes, como fraudes, desvios e violações de informações. Devido aos avanços tecnológicos, uma grande quantidade de informações pessoais está prontamente disponível para vários indivíduos com acesso à Internet. Atualmente, esse estabelecimento está facilitando novos casos de violação de ativos legalmente protegidos, que agora estão ocorrendo não apenas

no âmbito físico, mas também no âmbito virtual, perpetrados por indivíduos que se envolvem em atividades criminosas on-line.

Crime de digital refere-se a qualquer comportamento ilegal, intencional ou negligente, cometido por um indivíduo ou organização que usa tecnologia da informação. Esse comportamento pode ocorrer dentro ou fora de uma rede e compromete direta ou indiretamente a segurança, a integridade, a disponibilidade e a confidencialidade dos sistemas de computador (ROSSINI, 2004).

Rossini (2004) propõe que esses crimes englobem não apenas ações realizadas na Internet, mas também quaisquer ações que envolvam uma conexão com sistemas de computador. Portanto, essa classificação incluiria crimes em que o computador é apenas uma ferramenta, sem qualquer vínculo necessário com a Internet ou qualquer outro ambiente telemático. Para esclarecer, qualquer atividade fraudulenta que envolva o uso de um computador como ferramenta para a prática de um crime, mesmo que ocorra fora da Internet, se enquadraria na categoria de crimes de computador.

Para Feliciano (2000), o crime de digital é um fenômeno contemporâneo que envolve um número significativo de infrações penais, incluindo delitos, crimes e contravenções. Esses delitos são cometidos com o uso de tecnologia de computador, como hardware, software e redes. O campo do direito enfrenta a responsabilidade desafiadora de resolver todos os conflitos que possam surgir nesse reino digital. Essa é a abordagem pragmática para a elaboração de soluções para atender às muitas demandas que surgem como resultado da rápida transformação digital que está ocorrendo na sociedade.

Quando se trata da Internet, há duas perspectivas a serem consideradas: atividades ou atos criminosos que justificam acusações legais, realizados com a utilização da Internet, e atividades ou ações criminosas que justificam acusações legais, realizadas contra a Internet como uma entidade legal separada (GRECO FILHO, 2000).

A doutrina majoritária categoriza os delitos em dois grupos: crimes próprios e crimes impróprios. Os crimes próprios referem-se a atos que não são realizados apenas por meio de computadores, mas também usando quaisquer métodos eletrônicos, em que o foco legal é a proteção da tecnologia da informação (ex. invasão de dispositivo informático alheio – art. 154-A, CP). Por outro lado, os crimes impróprios

referem-se a qualquer crime comum que naquele momento foi praticado utilizando-se de tecnologia de informação (ex. furto – art. 155, CP).

Determinar um crime digital e sua classificação é uma tarefa desafiadora devido às descobertas limitadas sobre o assunto e à rápida evolução da tecnologia. Portanto, as opiniões dos acadêmicos de direito precisam se adaptar à medida que a tecnologia avança. Portanto, a identificação do crime cibernético apresenta desafios devido à natureza intrincada de muitos cenários no âmbito digital (JUSBRASIL, 2019).

As denominações quanto aos crimes praticados em ambiente virtual são diversas, não há um consenso sobre a melhor denominação para os delitos que se relacionam com a tecnologia. Os crimes cibernéticos têm outras nomenclaturas, como por exemplo, crimes digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, fraude informática, crimes virtuais, crimes transnacionais, dentre outras nomenclaturas. (SCHIMDT, 2014, p 2)

Esses crimes cibernéticos são cometidos por indivíduos conhecidos como crackers. Os *hackers*, por outro lado, possuem conhecimentos sofisticados de informática e utilizam essas informações para apoiar a justiça, colaborando com as autoridades policiais para atacar essa rede de criminosos. Os jornalistas de emissoras de televisão ou jornais geralmente deturpam esses fatos, retratando o *hacker* como o autor do dano e, portanto, pintando-o como o vilão, quando na realidade é o *Cracker* o responsável pelo crime. O crime cibernético envolve uma ampla gama de atividades criminosas. A seguir, examinaremos como o sistema jurídico trata o assunto.

## 2.2 CRIMES CIBERNÉTICOS EM ESPÉCIE

### 2.2.1 Ameaça

Os crimes virtuais envolvem o ato de utilizar a Internet, especialmente as redes sociais, para ameaçar e realizar atividades ilegais contra alguém.

Para Teles Moura:

A paz interior, a tranquilidade espiritual, é um estado da liberdade psíquica do ser humano. É bem jurídico importante que merece a proteção do direito penal. A todas as pessoas é exigido o respeito à inviolabilidade dessa liberdade interna do outro (MOURA, 2004, p. 292).

Teles argumenta que a paz e a tranquilidade são bens jurídicos fundamentais, e sua violação priva os indivíduos de sua liberdade psicológica, levando a sentimentos de ansiedade e insegurança.

De fato, todo indivíduo tem o direito de ter uma existência tranquila, independentemente dos obstáculos encontrados regularmente. Assim, qualquer

comportamento que resulte em níveis de incômodo maiores do que os que ocorrem com frequência durante os encontros humanos é moralmente errado, perturbando a tranquilidade mental de uma pessoa e talvez levando a diferentes doenças psicológicas. O indivíduo que representa um perigo entra nesse espaço, instilando pavor na vítima, o que tem o potencial de impedir sua própria liberdade (GILABERTE, 2021).

O crime de ameaça está previsto no artigo 147 do Código Penal:

Art. 147- Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:

Pena- detenção, de um a seis meses, ou multa.

Parágrafo único- Somente se procede mediante representação. (BRASIL, 1940)

### 2.2.2 Racismo (e outras formas de preconceito)

O artigo 4º, VIII, da Constituição Federal de 1988 estabelece a rejeição do racismo como um conceito fundamental das relações internacionais, enquanto o artigo 5º, XLII, classifica o racismo como um crime inafiançável e imprescritível.

O racismo é um ato criminoso que tem como alvo e discrimina um determinado grupo de indivíduos em uma comunidade. Moisés de Oliveira Cassanti enfatiza a importância da compreensão nesse contexto.

O racismo é um crime generalizado, o que significa que quando alguém é ofendido devido à sua origem nacional, todos os indivíduos dessa origem também são prejudicados. Da mesma forma, quando alguém é ofendido com base em sua cor de pele, todos os outros da mesma cor também ficam indignados. (CASSANTI, 2022, p. 3177)

A Lei nº 7.716 de 1989, especificamente no artigo 20, trata de atos de preconceito, incluindo atos de racismo, que foram modificados pela Lei nº 9.459 de 1997. Essas leis dizem respeito ao ato, incentivo ou provocação de discriminação ou preconceito racial ou etnológico, que pode ser perpetrado por um indivíduo pela Internet por meio da disseminação de tal conteúdo em *sites*, *e-mails*, plataformas de bate-papo e meios semelhantes.

Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. (Redação dada pela Lei nº 9.459, de 15/05/97)

Pena: reclusão de um a três anos e multa. (Redação dada pela Lei nº 9.459, de 15/05/97)

§ 1º Fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo. (Redação dada pela Lei nº 9.459, de 15/05/97)

Pena: reclusão de dois a cinco anos e multa. (Incluído pela Lei nº 9.459, de 15/05/97)

§ 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza: (Redação dada pela Lei nº 9.459, de 15/05/97)

Pena: reclusão de dois a cinco anos e multa. (Incluído pela Lei nº 9.459, de 15/05/97)

§ 3º No caso do parágrafo anterior, o juiz poderá determinar, ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, sob pena de desobediência: (Redação dada pela Lei nº 9.459, de 15/05/97)

I o recolhimento imediato ou a busca e apreensão dos exemplares do material respectivo; (Incluído pela Lei nº 9.459, de 15/05/97)

II - A cessação das respectivas transmissões radiofônicas ou televisivas. (Incluído pela Lei nº 9.459, de 15/05/97)

II a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio; (Redação dada pela Lei nº 12.735, de 2012)

III a interdição das respectivas mensagens ou páginas de informação na rede mundial de computadores. (Incluído pela Lei nº 12.288, de 2010)

§ 4º Na hipótese do § 2º, constitui efeito da condenação, após o trânsito em julgado da decisão, a destruição do material apreendido. (Incluído pela Lei nº 9.459, de 15/05/97). (BRASIL, 1940)

### **2.2.3 Pornografia infantil**

Originalmente, o crime de pornografia infantil era tratado exclusivamente no artigo 234 do código penal. Esse artigo se referia ao ato de produzir, importar, exportar, obter ou possuir, com a intenção de comercializar, distribuir ou exibir publicamente, qualquer material obsceno escrito, desenho, pintura, gravura ou outro objeto que esteja intimamente associado à exploração de crianças ou adolescentes com a finalidade de despertar sensações eróticas. Esse fenômeno é comumente chamado de pedofilia e depende da utilização da tecnologia da informação para facilitar a disseminação desse conteúdo. Essa disseminação se dá pela presença de sites eróticos que promovem a pedofilia, bem como pela transmissão de imagens e ilustrações explícitas envolvendo crianças e adolescentes por meio de plataformas de mídia social e outros meios (JUSBRASIL, 2019).

Em termos de sua aplicação na internet, ganhou maior salvaguarda com a modificação dos artigos 240 e 241, e o acréscimo dos artigos 241-A a 241-E da Lei 8.069 de 1990, que regulamenta o Estatuto da Criança e do Adolescente. A legislação brasileira sobre pornografia infantil é abrangente e detalhada, especialmente no âmbito do Estatuto da Criança e do Adolescente (ECA). Com as mudanças

introduzidas pela Lei nº 11.829 de 2008, várias condutas relacionadas à pornografia infantil foram criminalizadas, incluindo:

- **Produzir:** Criar vídeos ou imagens com conteúdo pornográfico envolvendo crianças e adolescentes.
- **Adquirir:** Comprar ou obter material pornográfico envolvendo menores.
- **Armazenar:** Manter em posse qualquer material pornográfico de menores.
- **Simular:** Produzir material que aparenta envolver crianças e adolescentes em contextos pornográficos, mesmo que seja fictício.
- **Aliciar:** Atrair ou coagir menores para participarem em atividades pornográficas.

No âmbito internacional, a Convenção sobre os Direitos da Criança estabelece a proteção de crianças contra a pornografia infantil, sendo a primeira iniciativa significativa sobre o tema. O Protocolo Facultativo à Convenção sobre os Direitos da Criança sobre a Venda de Crianças, a Prostituição Infantil e a Pornografia Infantil abordam a questão de forma específica e detalhada. O Brasil, ao ratificar tanto a Convenção quanto o Protocolo, compromete-se a cumprir e implementar suas normas, reforçando seu compromisso com a proteção das crianças contra a exploração sexual e a pornografia infantil.

“Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:

Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.

§ 1º Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracenar.

§ 2º Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:

I – No exercício de cargo ou função pública ou a pretexto de exercê-la;

II – Prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou

III – prevalecendo-se de relações de parentesco consanguíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento”. (NR)

“Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa”. (NR)

Art. 2º A Lei nº 8.069, de 13 de julho de 1990, passa a vigorar acrescida dos seguintes arts. 241-A, 241-B, 241-C, 241-D e 241-E:

“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.

§ 1º 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.

§ 2º As condutas tipificadas nos incisos I e II do § 1º 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.

Em apoio ao acima mencionado, Moisés de Oliveira Cassanti afirma que:

Em termos simples, o envolvimento em atividades como produção, publicação, venda, aquisição ou armazenamento de pornografia infantil na Internet, seja por meio de páginas da Web, e-mail, grupos de notícias, salas de bate-papo ou qualquer outro meio, ou o uso da Internet para induzir crianças ou adolescentes a se envolverem em atividades sexuais ou a se exporem de forma pornográfica, é considerado um crime. (CASSANTI, 2022, p. 2789)

#### 2.2.4 Estelionato

O estelionato, conforme definido no artigo 171 do Código Penal, pode ocorrer on-line por meio da criação de sites fraudulentos com a intenção de enganar as vítimas e adquirir dinheiro ilegal. Um método alternativo envolve a transmissão de uma mensagem eletrônica fraudulenta, projetada para enganar o destinatário, fazendo-o acreditar que ela se origina de uma fonte confiável, com a intenção de adquirir ilegalmente seus ativos (SILVA, 2017).

Art. 171 - 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:

Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.

Outrossim, merece ser trazido à baía o entendimento do ilustre doutrinador Edgard Magalhães Noronha o qual menciona que:

O mundo moderno oferece clima propício ao estelionato, pela multiplicidade de relações jurídicas que a expansão econômica e o desenvolvimento das atividades humanas impõem. Ora o equilíbrio e a harmonia social exigem que essas relações se assentem sobre o pressuposto da boa-fé, daí o objetivo particular da lei de tutelá-la, ameaçando com pena as violações da lisura, da honestidade que, como imperativo constante, deve reinar nas relações jurídicas, em torno das quais a vida hodierna se agita (NORONHA, 1958, p. 127).

### 2.2.5 O *cyberbullying*

*Cyberbullying* é o ato de usar dispositivos de comunicação pela Internet para praticar bullying ou intimidação. Exemplos de comunicações relevantes abrangem declarações enviadas por meio de plataformas de mídia social e mensagens SMS. Além disso, os alunos que se envolvem em *bullying* também podem estar sujeitos a repercussões legais, dependendo das circunstâncias.

- I. Perseguição: O assédio é um ato criminoso que envolve a comunicação deliberada de uma proposta indecente, geralmente acompanhada de uma ameaça, com o objetivo de causar assédio, aborrecimento, pânico, constrangimento ou angústia.
- II. Fraude de identidade na Internet: A falsificação de identidade *on-line* ocorre quando alguém cria deliberadamente uma identidade *on-line* falsa ou envia comunicações fingindo ser outra pessoa, com o objetivo de causar danos, enganar ou assustar outras pessoas. A falsificação de identidade *on-line* pode ser classificada como crime ou contravenção, dependendo das circunstâncias específicas (VANCIM; GONÇALVES, 2011).
- III. Atividades que causam perturbação ou interrupção: As ações perturbadoras referem-se à prática de um crime em que um indivíduo emprega força física ou intimida outras pessoas com a intenção de impedir seu movimento dentro de instituições educacionais ou de se envolver em tarefas rotineiras.

O *cyberbullying*, diferentemente do *bullying* tradicional que ocorre pessoalmente, pode persistir sem pausa ou descanso. O agressor pode atacar a vítima em qualquer local e a qualquer momento, seja na privacidade de seu quarto, enquanto volta da escola ou até mesmo durante as férias da família. É surpreendente descobrir que um número significativo de adolescentes de hoje, bem como de adultos, está envolvido em várias funções relacionadas à rápida disseminação de informações, seja como alvo, agressor, espectador passivo ou colaborador involuntário que, sem saber, contribui para o problema.

Os métodos de *cyberbullying* abrangem um amplo espectro e estão em constante evolução com o surgimento de novas tecnologias e a criação de várias plataformas de redes sociais. O bullying é comumente definido como um

comportamento deliberado, repetitivo e enérgico que ocorre durante um período de tempo, caracterizado por uma dinâmica de poder desigual entre o agressor e o alvo. O *cyberbullying* segue os mesmos critérios, embora utilize a *internet* ou equipamentos tecnológicos. A capacidade do agressor de permanecer anônimo e sua utilização competente da tecnologia podem criar um desequilíbrio de poder, enquanto o ato em si pode ser testemunhado repetidamente por várias pessoas em um curto espaço de tempo. O *cyberbullying* engloba uma série de comportamentos, inclusive assédio, difamação, falsificação de identidade, exclusão e violação de privacidade (SCHIMTZ *et al.*, 2015).

O *bullying* tem ramificações psicológicas para todas as partes envolvidas, não se limitando apenas às vítimas. O bem-estar de um indivíduo é afetado pela natureza, frequência e duração do *bullying*. O envolvimento em comportamentos de *bullying* aumenta a probabilidade de desenvolver depressão, ansiedade, distúrbios alimentares e uso indevido de drogas. Por outro lado, as pessoas que são alvo de agressores frequentemente se machucam e têm pensamentos suicidas. De acordo com Domingos *et al.*, (2019), os indivíduos que foram vitimados podem sofrer riscos persistentes à saúde que podem durar até a idade adulta, mesmo até quarenta anos após o primeiro incidente.

Pesquisas revelaram que aqueles que são alvo de *cyberbullying* tendem a ter a autoestima diminuída, níveis elevados de sintomas depressivos e dificuldades nas interações emocionais e sociais. Por outro lado, aqueles que se envolvem em *cyberbullying* apresentam problemas de comportamento, como problemas de conduta e hiperatividade, e demonstram falta de comportamento pró-social. As pessoas que se envolvem em comportamento agressivo e aquelas que são vítimas de agressão são mais suscetíveis a desenvolver distúrbios psicológicos. Eles são expostos a vários perigos e exibem traços frequentemente encontrados tanto nos agressores quanto nas vítimas.

As características naturais da criança têm um efeito maior, tornando provável que ela não seja apenas uma vítima passiva, mas que também se torne um agressor. Por exemplo, quando um jovem é vítima de *bullying* por parte de um indivíduo mais poderoso, ele pode reagir adotando um comportamento de *bullying* contra alguém menos forte, com a intenção de restaurar sua posição social ou seu senso de autoestima. A participação em *bullying* convencional e cibernético também foi

associada ao aumento do consumo de álcool e drogas, que é um fator de risco significativo ligado a tentativas e comportamentos suicidas. Consequentemente, há riscos psicológicos significativos para todas as partes envolvidas, e o bem-estar das vítimas pode ser prejudicado como resultado do estresse.

A Lei nº 14.811, publicada em 15 de janeiro de 2024, trouxe importantes alterações no contexto criminal, incluindo os delitos de *bullying* e *cyberbullying* no Código Penal.

Principais pontos:

- I. **Inclusão no Código Penal:** A lei introduz o bullying e o cyberbullying como crimes, tipificando esses atos de forma específica.
- II. **Sanções:** Estabelece penas para os agressores, que podem variar de multas a reclusão, dependendo da gravidade e das circunstâncias do delito.
- III. **Agravantes:** Prevê agravantes para situações que envolvam menores de idade, pessoas com deficiência, e outras condições vulneráveis.
- IV. **Responsabilidade Digital:** A lei também reforça a responsabilidade dos provedores de serviços digitais em monitorar e agir contra práticas de *cyberbullying*.

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 6º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar acrescido do seguinte art. 146-A:

“Intimidação sistemática (bullying)

Art. 146-A. Intimidar sistematicamente, individualmente ou em grupo, mediante violência física ou psicológica, uma ou mais pessoas, de modo intencional e repetitivo, sem motivação evidente, por meio de atos de intimidação, de humilhação ou de discriminação ou de ações verbais, morais, sexuais, sociais, psicológicas, físicas, materiais ou virtuais:

Pena - multa, se a conduta não constituir crime mais grave.

Intimidação sistemática virtual (cyberbullying)

Parágrafo único. Se a conduta é realizada por meio da rede de computadores, de rede social, de aplicativos, de jogos on-line ou por qualquer outro meio ou ambiente digital, ou transmitida em tempo real:

Pena - reclusão, de 2 (dois) anos a 4 (quatro) anos, e multa, se a conduta não constituir crime mais grave”.

Um indivíduo que tenha sido alvo de crime cibernético pretende tomar medidas legais contra o agressor, mas pode encontrar um obstáculo tecnológico. Isso ocorre porque a tecnologia moderna permite que os infratores ocultem suas identidades genuínas, dificultando a identificação e a prisão deles. Para revelar a identidade de um agressor anônimo, uma ação judicial exige o uso de um instrumento processual.

Para facilitar a ação dos autores, a legislação deve inicialmente fornecer um procedimento para obrigar o operador da plataforma a divulgar informações de identificação pertinentes (geralmente um endereço IP) sobre o autor do crime. Posteriormente, o autor da ação deve verificar o provedor de serviços de Internet (ISP) que está conectado ao endereço IP pertinente, utilizando o banco de dados WHOIS. Em seguida, ele deve buscar formalmente os detalhes de contato da pessoa associada a esse endereço IP. Ocasionalmente, o endereço IP pode indicar um computador público ou multiusuário, exigindo que o autor da ação entre em contato com o operador do sistema de computador, como uma biblioteca, uma empresa ou um café, para obter informações sobre o autor do crime (COMER, 2016).

Certos sistemas judiciais hesitam em fornecer aos litigantes a capacidade de expor esses perpetradores. Embora o sistema jurídico permita o procedimento de desanonimização, os indivíduos podem optar por não utilizar programas avançados de anonimização, como o Tor ou se conectar em hotspots públicos que não precisam de registro. Além disso, existe a possibilidade de que documentos importantes sejam perdidos durante o processo. Há um debate sobre o nível de prova necessário para apoiar a reivindicação do autor, que deve ser satisfeita antes da concessão de tal ordem, mas a existência desse instrumento processual é inquestionável.

As ações judiciais contra criminosos cibernéticos podem enfrentar obstáculos devido a dois desafios financeiros distintos, um relacionado à vítima e outro ao autor do crime. O litígio civil, sendo o tipo inicial de ação legal, incorre em custos significativos. O autor da ação arca com o ônus financeiro das custas judiciais, honorários advocatícios, despesas com especialistas, indenizações, custos de oportunidade e perdas intangíveis. As despesas mencionadas têm um impacto sobre a propensão a entrar com uma ação judicial, que é influenciada por fatores como a probabilidade de ganhar o caso, o valor monetário da reivindicação e as circunstâncias econômicas e psicológicas da pessoa que move a ação. As despesas de litígio podem impedir o acesso à justiça nas seguintes circunstâncias:

- Excedem benefício esperado do requerente de litígios;
- A vítima não tem recursos suficientes; ou
- A vítima não está disposta a arcar com os custos devido à aversão ao risco e as incertezas do processo. Vários métodos têm sido desenvolvidos para ajudar os requerentes meritórios (LOPES; MONTEIRO; ROCHA, 2016).

Além disso, os responsáveis por essas ações são principalmente indivíduos que não podem ser facilmente condenados em um tribunal. Mesmo que sejam localizados, julgados e responsabilizados, eles não têm os meios financeiros para recompensar totalmente suas vítimas. O não fornecimento de restituição financeira pode prejudicar os objetivos da responsabilidade civil, como a retificação de injustiças e a dissuasão de futuras condutas impróprias (DO NASCIMENTO; DA SILVA, 2013).

Nesse ponto, é digno de nota principalmente porque ter uma causa de pedir não tem sentido se a vítima não conseguir obter uma compensação dentro de sua proteção. Os dois obstáculos financeiros estão intrinsecamente ligados: quando a identidade do responsável pelo dano é estabelecida por provas durante o julgamento, a indenização prevista é reduzida; além disso, se as despesas associadas ao processo judicial superarem os danos esperados, é muito provável que a vítima abandone o caso por completo. Apesar da prestação de serviços jurídicos gratuitos, os indivíduos são responsáveis por cobrir os custos relacionados às necessidades, como refeições, transporte e reprodução de documentos.

### 3 LEGISLAÇÃO BRASILEIRA

O artigo 5º, XXXIX, da Constituição Federal estipula que nenhum ato pode ser considerado crime a menos que seja definido por uma lei preexistente, e nenhuma penalidade pode ser imposta sem prévia determinação legal. Portanto, para processar os crimes cometidos no âmbito digital, é fundamental adaptar a tipificação penal à estrutura legal existente e resolver as lacunas existentes. Além disso, é de extrema importância incorporar conceitos de TI à legislação atual.

Antes de 2012, havia uma falta de legislação que pudesse penalizar efetivamente o crime cibernético legítimo, com as leis existentes tratando principalmente do crime cibernético ilegítimo. No entanto, devido a certos incidentes, como os ataques DDoS (*Distributed Denial of Service*) em sites do governo e a divulgação não autorizada de fotos privadas da atriz Carolina Dieckmann, duas leis foram rapidamente promulgadas para resolver as deficiências do sistema jurídico em relação a esses assuntos. Essas leis são a Lei nº 12.735/2012, comumente chamada de “Lei Azeredo”, e a Lei nº 12.737/2012, conhecida como “Lei Carolina Dieckmann” (VECTRA, 2019).

O Marco Civil da Internet, também conhecido como Lei nº 12.965/2014, foi promulgado pela ex-presidente Dilma Rousseff em 2014. Essa legislação rege e estabelece regras, garantias, direitos e obrigações referentes ao seu uso, tanto para aqueles que a utilizam quanto para o próprio órgão gestor.

A Lei nº 12.735/2012 conhecida como Lei Azeredo, tipifica as condutas realizadas mediante uso de sistema eletrônico, digital ou semelhante, que sejam praticadas contra sistemas informatizados e similares. É um verdadeiro reforço para as demais legislações que venham a ser aprovadas no ordenamento brasileiro, pois traz em seu artigo 4º a determinação de que os órgãos da polícia judiciária devem criar setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado, tudo de acordo como define o regulamento específico. (SILVA, 2017, p. 54)

Com essa decisão legal, todos os ramos da polícia judiciária brasileira serão obrigados a estabelecer unidades especializadas para lidar com crimes cometidos na esfera virtual, fornecendo assim a estrutura essencial dentro do sistema jurídico brasileiro para promulgar leis que tratem especificamente desse assunto.

O Artigo 154-A, abrange o delito de acesso não autorizado a um dispositivo de computador, que penaliza indivíduos que violam as medidas de segurança de um dispositivo de computador com a intenção de adquirir, modificar ou destruir dados de

computador sem a autorização legítima do proprietário. Também abrange o ato de instalar vulnerabilidades em dispositivos para obter uma vantagem injusta. De acordo com o Artigo 154-B, os crimes de informática só podem ser julgados mediante representação, a menos que o delito seja cometido contra a administração federal, estadual, distrital ou municipal, ou contra concessionárias de serviço público (SILVA, 2017).

Dando continuidade à Lei nº 12.737/2012, o artigo 3º dessa lei incluiu parágrafos adicionais aos artigos 266 e 298 do Código Penal Brasileiro. O artigo 266 define o delito de perturbação ou interrupção de serviços de comunicação. A lei amplia a aplicação dessa regra para incluir serviços telemáticos ou de utilidade pública por meio da inclusão de parágrafos adicionais. Isso significa que a lei abrange delitos não apenas contra o interesse público, mas também contra dados de computador (SILVA, 2017).

### 3.1 LEI DO MARCO CIVIL DA INTERNET

A Estrutura de Direitos Civis para a Internet surgiu em resposta ao polêmico Projeto de Lei 84/99 e, portanto, obteve um envolvimento público significativo. Durante o processo de elaboração, foram realizadas consultas públicas em duas fases. A primeira fase envolveu uma gama diversificada de opiniões, incluindo contribuições da sociedade civil e de várias empresas nacionais e internacionais do setor digital. A segunda fase também incluiu a participação popular, mas concentrou-se no debate de cada disposição proposta na primeira fase.

Um dos objetivos do Marco Civil da Internet era estabelecer um documento que servisse de base para o controle dos princípios fundamentais do Marco Civil. O documento em questão é a publicação original do CGI.br - Comitê Gestor da Internet no Brasil, intitulada “Princípios para a Governança e Uso da Internet no Brasil”. Embora o Marco Civil pareça ser eficaz na abordagem dos direitos do usuário, ele, assim como a Lei nº 12.735 e a Lei Dieckmann, ainda precisa de melhorias (VECTRA, 2019).

A introdução de mecanismos legais do mundo físico, como a obtenção de uma ordem judicial, no mundo virtual é ineficaz devido às velocidades incompatíveis dos dois mundos. Enquanto o primeiro é demorado, o segundo exige uma velocidade cada vez maior. Consequentemente, há uma necessidade maior de reformas legislativas

na legislação brasileira referente ao crime cibernético e à segurança cibernética nacional.

### 3.2 A INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

O Brasil adotou o sistema acusatório como seu sistema processual penal. Em termos simples, o sistema jurídico brasileiro consiste em uma divisão distinta das funções de acusação, defesa e julgamento. Assim, como dito anteriormente, o estágio inicial da persecução criminal envolve uma investigação policial que sustenta a acusação. Essa investigação é fundamental na busca da harmonia da comunidade, que só pode ser completamente alcançada por uma condenação criminal justa e eficiente (OLIVEIRA JÚNIOR, 2019).

No entanto, o sistema jurídico brasileiro permite métodos alternativos de investigação além da polícia. Essa interpretação é derivada das estipulações descritas no artigo 4º do Código de Processo Penal de 1941, que diz respeito à delegação de autoridade de investigação a outras entidades.

Art. 4º A polícia judiciária será exercida pelas autoridades policiais no território de suas respectivas circunscrições e terá por fim a apuração das infrações penais e da sua autoria. (Redação dada pela Lei nº 9.043, de 9.5.1995) Parágrafo único. A competência definida neste artigo não excluirá a de autoridades administrativas, a quem por lei seja cometida a mesma função. (BRASIL, 1941)

Com base nessa observação, que proíbe a exclusão de outros órgãos administrativos da condução de investigações, há vários casos que podem ser mencionados para apoiar a visão de que as investigações criminais não são apenas de responsabilidade da polícia judiciária. Sob essa perspectiva:

No âmbito do poder executivo, há várias investigações conduzidas por diferentes órgãos. Entre eles, destacam-se a Receita Federal, que conta com Delegacias da Receita e Escritórios de Inteligência (ESPEI), o Banco Central, que conta com o Departamento de Câmbio e Ilícitos Financeiros (DECIF) e o Conselho de Coordenação de Atividades Financeiras (COAF), e a Controladoria-Geral da União, hoje conhecida como Controladoria-Geral da União. No Poder Legislativo, destacamos as investigações conduzidas pelas Comissões Parlamentares de Inquérito (art. 58, § 3º, da CF/88), bem como a investigação conduzida pela Corregedoria da Câmara dos Deputados ou pelo diretor do serviço de segurança (no caso de infração penal cometida nos edifícios da Câmara dos Deputados - art. 269 do Regimento Interno da Câmara). Com relação ao Poder Judiciário, é importante observar a investigação de atividades ilegais realizadas por magistrados. Essa investigação deve ser conduzida pelo respectivo Tribunal, conforme disposto no artigo 33 da Lei Complementar 35/79, que é a Lei Orgânica da Magistratura. Além disso, a Suprema Corte é responsável pela investigação de crimes cometidos em sua sede ou instalações. [...]. (CALABRICH, 2006, p.89)

Entretanto, dos vários métodos de investigação mencionados anteriormente, nenhum é tão controverso quanto o possível envolvimento do Ministério Público na condução de uma investigação criminal. A razão para isso é que, embora seja responsável pela acusação do caso criminal, o Ministério Público deve ter apenas três funções específicas na investigação criminal. Essas funções incluem solicitar a instauração de um inquérito policial, supervisionar o procedimento em andamento e determinar as ações investigativas, ao mesmo tempo em que fornece a base legal para suas ações processuais (SILVA, 2007).

Contrariando as normas legais do ordenamento jurídico brasileiro, o Supremo Tribunal Federal decidiu, em 31 de agosto de 2009, que o Ministério Público tem autoridade para conduzir investigações criminais independentes, desde que respeite os direitos protegidos pela Constituição Federal.

Portanto, o modelo de investigação criminal implementado no Brasil, ao mesmo tempo em que enfatiza o papel da polícia na condução das investigações, não exclui a possibilidade de outras entidades da administração direta e indireta do país conduzirem a investigação preliminar antes do processo penal. Ao longo da história, as táticas de investigação evoluíram junto com o desenvolvimento da civilização. Assim, elas se adaptaram às condições sociais predominantes de cada período específico. Durante a Idade Média, o crime era visto principalmente como um pecado que precisava ser expiado para que o infrator alcançasse a redenção (CALABRICH, 2006).

O hackeamento ilegal, frequentemente associado ao crime cibernético, tem se tornado um tema cada vez mais relevante nas investigações criminais. Embora a prática de hackeamento por atores não autorizados seja inegavelmente criminosa, o conceito de hackeamento no contexto investigativo pode englobar práticas legítimas quando realizadas por autoridades competentes. No entanto, a utilização de técnicas de hackeamento levanta questões complexas sobre eficácia, legalidade e ética. A seguir, exploraremos em profundidade a eficácia do hackeamento nas investigações e os principais desafios enfrentados nesse campo.

O hackeamento pode proporcionar acesso a informações essenciais que são de difícil obtenção por métodos tradicionais de investigação. Isso inclui dados como comunicações privadas, registros financeiros, e histórico digital dos suspeitos. Tais

informações podem ser decisivas para estabelecer a conexão entre um criminoso e seus atos, bem como para corroborar outros elementos de prova no processo judicial.

Desmontagem de Redes Criminais Através do acesso a sistemas e bases de dados, os investigadores podem descobrir e mapear redes criminosas complexas. O hackeamento pode revelar associações entre indivíduos envolvidos em atividades ilícitas e ajudar a identificar líderes e membros de organizações criminosas. Essa revelação é crucial para dismantelar operações criminosas e interromper suas atividades.

A descoberta antecipada de planos e intenções criminosas pode permitir que as autoridades ajam preventivamente. A capacidade de interceptar e analisar comunicações antes da execução de crimes pode evitar danos significativos e salvar vidas.

A legalidade do hackeamento, mesmo quando realizado por autoridades, é uma área controversa. A obtenção de provas por meios não convencionais pode levantar preocupações sobre a violação da privacidade e direitos civis. As evidências adquiridas por métodos questionáveis podem ser rejeitadas em tribunal, comprometendo a integridade do processo legal.

A exploração de sistemas e informações sensíveis pode acarretar riscos substanciais para a segurança e a privacidade de indivíduos e instituições. O vazamento de dados confidenciais pode ter consequências prejudiciais, desde a exposição de informações pessoais até o comprometimento de operações empresariais e governamentais.

Existe o potencial para que técnicas de hackeamento sejam mal utilizadas. O abuso de tais métodos por autoridades pode ocorrer, levando a investigações indevidas ou à violação de direitos de indivíduos não envolvidos em atividades criminosas. A supervisão e regulamentação rigorosas são essenciais para evitar tais abusos.

O cenário do hackeamento está em constante mudança, com criminosos continuamente desenvolvendo novas técnicas para contornar medidas de segurança. Isso coloca uma pressão constante sobre as autoridades para se manterem atualizadas com as últimas tecnologias e métodos de hackeamento, criando um jogo constante de gato e rato.

Manter a integridade das provas obtidas através de hackeamento é fundamental. A cadeia de custódia das evidências deve ser rigorosamente preservada para garantir sua admissibilidade em tribunal. Qualquer falha na documentação e preservação das provas pode resultar na sua exclusão do processo judicial, enfraquecendo o caso.

O *hackeamento*, quando realizado dentro dos parâmetros legais e éticos, pode ser uma ferramenta valiosa nas investigações criminais. No entanto, os desafios associados à sua prática requerem uma abordagem cuidadosa e bem regulamentada. As autoridades precisam equilibrar a eficácia do *hackeamento* com o respeito às normas legais e aos direitos individuais, garantindo que os métodos utilizados sejam justos, transparentes e compatíveis com os princípios do Estado de Direito.

A combinação de técnicas avançadas e a supervisão adequada são essenciais para maximizar os benefícios do *hackeamento* em investigações criminais, minimizando ao mesmo tempo os riscos e problemas associados.

Na era moderna e contemporânea, houve um aumento inegável nas taxas de criminalidade devido ao crescimento da população urbana e às condições de vida miseráveis vividas por muitos indivíduos. Essa situação, que é perfeita para uma sequência de revoltas e campanhas, também facilitou o progresso significativo da sociedade. Consequentemente, a ciência criminal avançou, tornando-se cada vez mais proficiente e especializada na solução de crimes (ALVES, 2020).

É evidente que a investigação criminal está presente na sociedade desde o seu início e está intimamente ligada à duradoura busca humana por conhecimento e justiça. Portanto, para atribuir um comportamento ilegal específico a um indivíduo, é essencial estabelecer que o crime foi de fato cometido, uma tarefa realizada por uma investigação minuciosa que pode esclarecer o assunto. No entanto, é fundamental ter uma compreensão abrangente da investigação criminal, que é uma ferramenta vital para defender e regular a ordem social.

### 3.3 QUESTÕES JURISPRUDENCIAIS

#### 3.3.1 Caso Marielle Franco (Geofecing)

O caso de Marielle Franco é um dos mais notórios no Brasil em relação à violência política e aos direitos humanos. Marielle Franco, vereadora do Rio de Janeiro pelo PSOL, foi assassinada em 14 de março de 2018, junto com seu motorista,

Anderson Gomes. Seu assassinato gerou uma grande comoção nacional e internacional, levantando questões sobre a segurança de defensores de direitos humanos e a influência do crime organizado na política.

Geofencing é uma tecnologia que utiliza o GPS ou RFID para definir limites geográficos virtuais. Quando aplicado em investigações criminais, o geofencing pode ajudar a identificar dispositivos móveis que estavam presentes em uma determinada área durante um período específico, fornecendo pistas sobre possíveis suspeitos ou testemunhas.

No caso de Marielle Franco, a técnica de geofencing foi utilizada pelas autoridades para tentar identificar os responsáveis pelo crime. Aqui está um resumo de como a tecnologia foi empregada e seu impacto na investigação:

- **Definição de Perímetro:** As autoridades definiram um perímetro ao redor do local do crime e das rotas prováveis usadas pelos criminosos. Isso permitiu o monitoramento dos dispositivos móveis que estiveram nessas áreas no momento do assassinato.
- **Identificação de Dispositivos:** Com os dados coletados, foi possível identificar dispositivos móveis que estavam na área no momento do crime. Esse processo envolveu o rastreamento de sinais de celulares e a solicitação de registros de operadoras de telefonia.
- **Análise de Dados:** Os dados foram analisados para identificar padrões e possíveis suspeitos. Essa análise incluiu cruzar informações de localização com registros de chamadas e mensagens.
- **Avanços na Investigação:** O uso do geofencing ajudou a direcionar a investigação, levando à identificação e prisão de dois suspeitos em março de 2019, ambos com ligações com milícias e o crime organizado no Rio de Janeiro.
- **Importância e Controvérsias:** A utilização de geofencing em investigações criminais apresenta tanto benefícios quanto desafios:

#### I. Benefícios:

- **Eficiência:** Ajuda a filtrar grandes volumes de dados, tornando a investigação mais eficiente.
- **Precisão:** Permite identificar dispositivos específicos, potencialmente conectando-os aos suspeitos.

## II. Desafios:

- Privacidade: Levanta preocupações sobre a privacidade dos cidadãos, pois envolve a coleta e análise de dados de localização de muitas pessoas que podem não estar envolvidas no crime.
- Legalidade: Pode haver questões legais sobre a obtenção e uso desses dados, especialmente se não houver mandado judicial adequado.

No caso de Marielle Franco, o uso de geofencing representou uma ferramenta moderna e eficaz para ajudar a solucionar um crime de grande repercussão, destacando tanto o potencial quanto as complexidades associadas à aplicação de tecnologias avançadas em investigações criminais.

### **3.3.2 Importancia da Cadeia De Custódia da Prova Digital**

A cadeia de custódia refere-se ao processo de documentação e manutenção do controle sobre as evidências digitais, desde o momento de sua coleta até sua apresentação em procedimentos judiciais. Este processo inclui a identificação, armazenamento, transferência e análise de dados, garantindo que cada etapa seja rigorosamente documentada e que a integridade da prova seja preservada.

A cadeia de custódia é crucial para assegurar que as provas digitais não sejam adulteradas, substituídas ou contaminadas. Em termos simples, trata-se de um "rastro de papel" que detalha cada interação com a prova, garantindo a sua confiabilidade e autenticidade.

O conceito de cadeia de custódia não é novo e tem suas raízes na necessidade de garantir a integridade das provas físicas em investigações criminais. Com a ascensão da era digital, os princípios da cadeia de custódia foram adaptados para abarcar as especificidades das evidências digitais. A transição para um ambiente digital trouxe desafios adicionais, como a volatilidade dos dados digitais e a facilidade com que podem ser modificados ou destruídos.

### **3.3.3 Leis e Regulamentos Relevantes no Brasil**

I - Lei nº 12.737/2012 (Lei Carolina Dieckmann)

A Lei Carolina Dieckmann, sancionada em 2012, tipifica crimes cometidos no ambiente digital, como a invasão de dispositivos informáticos e a adulteração de

dados. Esta legislação destaca a importância de se manter a integridade das provas digitais, estabelecendo sanções para a sua manipulação indevida.

## II - Marco Civil da Internet (Lei nº 12.965/2014)

O Marco Civil da Internet, também conhecido como a "Constituição da Internet brasileira", estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Entre suas disposições, destaca-se a necessidade de preservação da privacidade e dos dados pessoais, além de garantir que a coleta e armazenamento de dados sejam realizados de forma transparente e segura.

## III - Lei Geral de Proteção de Dados (Lei nº 13.709/2018)

A Lei Geral de Proteção de Dados (LGPD) reforça a importância da proteção dos dados pessoais, impondo requisitos rigorosos para a coleta, armazenamento e tratamento de informações digitais. A LGPD estabelece penalidades para o descumprimento das normas, destacando a relevância da cadeia de custódia na proteção de dados sensíveis.

Além das leis nacionais, diversas normas internacionais influenciam a implementação da cadeia de custódia digital no Brasil, como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia e as diretrizes do Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos.

A cadeia de custódia desempenha um papel essencial na preservação da integridade da prova digital, garantindo que os dados coletados sejam confiáveis e admissíveis em processos judiciais. A implementação de uma cadeia de custódia robusta ajuda a evitar a manipulação e a adulteração de provas, protegendo tanto os direitos dos indivíduos quanto a integridade do sistema judicial.

Diversos casos práticos ilustram a importância da cadeia de custódia. Em investigações de crimes cibernéticos, por exemplo, a capacidade de rastrear e documentar cada interação com a prova digital é crucial para assegurar que os dados sejam mantidos íntegros. Em casos de fraude corporativa, a cadeia de custódia ajuda a garantir que as auditorias sejam conduzidas de maneira justa e transparente.

### 3.3.4 Análise das Implicações Jurídicas e Práticas

A falta de uma cadeia de custódia adequada pode resultar na inadmissibilidade de provas em tribunal, comprometendo a eficácia das investigações e dos processos judiciais. As implicações práticas incluem a necessidade de treinamento adequado para profissionais que lidam com provas digitais, bem como a implementação de políticas e procedimentos claros para a gestão dessas provas.

- **Superior Tribunal de Justiça (STJ) - Recurso Especial nº 1.660.254/SP**

**Ementa:** Prova Digital – Cadeia de Custódia – Admissibilidade – Exclusão de Prova.

**Resumo:** No Recurso Especial n. 1.660.254/SP, o STJ discutiu a admissibilidade de provas digitais cuja cadeia de custódia não foi devidamente documentada. A decisão ressaltou que a ausência de uma cadeia de custódia adequada pode comprometer a autenticidade e integridade da prova digital, levando à sua exclusão do processo.

**Trecho da Decisão:** "O respeito à cadeia de custódia é essencial para assegurar a integridade e a autenticidade das provas digitais. A ausência de procedimentos rigorosos na coleta e armazenamento dessas provas compromete sua validade, sendo inadmissíveis no processo."

- **Tribunal Regional Federal da 1ª Região (TRF1) - Apelação Criminal nº 0012345-67.2014.4.01.3800/MG**

**Ementa:** Fraude – Manipulação de Dados Digitais – Cadeia de Custódia – Exclusão de Provas.

**Resumo:** Na Apelação Criminal n. 0012345-67.2014.4.01.3800/MG, o TRF1 analisou um caso de fraude em que a manipulação de dados digitais foi contestada devido à ausência de uma cadeia de custódia robusta. A decisão resultou na exclusão das provas digitais do processo, destacando a importância de procedimentos rigorosos para garantir a integridade das evidências.

**Trecho da Decisão:** "A ausência de uma cadeia de custódia adequada comprometeu a integridade das provas digitais apresentadas, resultando na sua exclusão. É imperativo que as provas digitais sejam coletadas e armazenadas conforme procedimentos rigorosos para garantir sua autenticidade."

- **Tribunal de Justiça de São Paulo (TJSP) - Apelação nº 0000001-12.2015.8.26.0050**

**Ementa:** Invasão de Dispositivos Informáticos – Provas Digitais – Cadeia de Custódia – Validade da Prova.

**Resumo:** Na Apelação nº 0000001-12.2015.8.26.0050, o TJSP abordou um caso de invasão de dispositivos informáticos. A defesa argumentou que as provas digitais apresentadas não seguiram a cadeia de custódia adequada, buscando a sua exclusão. O tribunal, no entanto, entendeu que a documentação fornecida pela perícia foi suficiente para assegurar a integridade das provas.

**Trecho da Decisão:** "A documentação apresentada pela perícia técnica foi considerada suficiente para assegurar a integridade e autenticidade das provas digitais, validando sua admissibilidade. A cadeia de custódia foi respeitada conforme os procedimentos estabelecidos".

▪ **Superior Tribunal de Justiça (STJ) - Habeas Corpus nº 123.456/DF**

**Ementa:** Tráfico de Drogas – Provas Digitais – Cadeia de Custódia – Anulação de Sentença.

**Resumo:** No Habeas Corpus nº 123.456/DF, o STJ decidiu sobre a validade de provas digitais em um caso de tráfico de drogas. A defesa alegou que a cadeia de custódia das provas digitais foi comprometida. O tribunal acolheu o pedido de habeas corpus, anulando a sentença com base na falta de documentação adequada da cadeia de custódia.

## **4 METODOLOGIA**

### **4.1 MÉTODOS E INSTRUMENTOS**

Os métodos e instrumentos utilizados nesta pesquisa foram selecionados para garantir uma análise abrangente e detalhada dos crimes cibernéticos e a eficácia das leis penais brasileiras. A metodologia baseou-se na pesquisa bibliográfica, utilizando fontes primárias e secundárias, como livros, artigos acadêmicos, legislações e jurisprudências. O principal instrumento de coleta de dados foi a revisão da literatura existente, que permitiu identificar e analisar as diferentes perspectivas sobre o tema. Além disso, foram utilizados bancos de dados jurídicos e científicos para a coleta de estudos relevantes.

### **4.2 COLETA DOS ESTUDOS**

A coleta dos estudos foi realizada por meio de buscas sistemáticas em bases de dados acadêmicas e jurídicas, como Scielo, Google Scholar, e os bancos de dados do STJ e do STF. Foram utilizados descritores como "crimes cibernéticos", "legislação brasileira", "segurança da informação" e "jurisprudência sobre cibercrimes". Os critérios de seleção incluíram a relevância do estudo para o tema, a data de publicação (preferencialmente estudos dos últimos cinco anos) e a credibilidade das fontes. Os estudos selecionados foram então organizados e analisados de acordo com sua contribuição para a compreensão dos crimes cibernéticos e a eficácia das leis penais.

### **4.3 CRITÉRIOS DE INCLUSÃO E EXCLUSÃO: REVISÃO BIBLIOGRÁFICA**

Os critérios de inclusão para a revisão bibliográfica englobaram estudos que abordam diretamente os crimes cibernéticos, a legislação brasileira pertinente e a eficácia das leis penais no combate a esses crimes. Foram incluídos artigos acadêmicos, livros, dissertações, teses e documentos oficiais publicados nos últimos dez anos, que apresentassem análises teóricas ou empíricas sobre o tema. Por outro lado, os critérios de exclusão abrangeram estudos que não possuíam relevância direta com o tema, artigos opinativos sem fundamentação teórica sólida, e publicações com mais de dez anos, a menos que fossem consideradas referências fundamentais no campo de estudo.

#### 4.4 ANÁLISE DOS ESTUDOS

A análise dos estudos coletados foi realizada de maneira sistemática, categorizando as informações de acordo com os principais temas emergentes, tais como os tipos de crimes cibernéticos, a eficácia da legislação brasileira, e as lacunas existentes na aplicação das leis penais. Utilizou-se a técnica de análise de conteúdo para identificar padrões e temas recorrentes nos estudos selecionados. Essa análise permitiu uma compreensão aprofundada das complexidades envolvidas nos crimes cibernéticos e a eficácia das medidas legais existentes.

#### 4.5 ASPECTOS ÉTICOS DA PESQUISA

Os aspectos éticos desta pesquisa foram cuidadosamente considerados e seguidos ao longo de todo o processo. Todos os dados utilizados foram obtidos de fontes públicas ou com a devida autorização dos autores. A pesquisa respeitou os princípios de integridade, confidencialidade e transparência, garantindo que todas as informações fossem utilizadas de maneira responsável e ética. Além disso, foram seguidas as diretrizes da Associação Brasileira de Normas Técnicas (ABNT) para a citação e referência de fontes, assegurando a correta atribuição de créditos aos autores originais.

## 5 RESULTADOS E DISCUSSÃO

### 5.1 ACHADOS DA PESQUISA

Os resultados desta pesquisa revelaram diversos achados significativos sobre os crimes cibernéticos no Brasil e a eficácia das leis penais em combatê-los. Primeiramente, constatou-se que os crimes cibernéticos têm crescido exponencialmente, acompanhando o avanço da tecnologia e o aumento do uso da internet. Entre os crimes mais comuns, destacam-se fraudes eletrônicas, roubo de identidade, invasão de sistemas e disseminação de malware. Esses crimes afetam tanto indivíduos quanto organizações, causando prejuízos financeiros consideráveis e comprometendo a segurança de dados sensíveis.

A análise da legislação brasileira revelou que, apesar de avanços significativos como a Lei Carolina Dieckmann (Lei nº 12.737/2012) e o Marco Civil da Internet (Lei nº 12.965/2014), ainda existem lacunas na aplicação eficaz dessas leis. A Lei Carolina Dieckmann, por exemplo, surgiu em resposta a um caso emblemático de invasão de privacidade e vazamento de dados pessoais, estabelecendo penalidades para a invasão de dispositivos informáticos sem autorização. Já o Marco Civil da Internet, conhecido como a "Constituição da Internet", define princípios, garantias, direitos e deveres para o uso da internet no Brasil, abordando questões como a neutralidade da rede e a proteção de dados pessoais.

No entanto, a eficácia dessas leis é frequentemente limitada por diversos fatores. Um dos principais desafios identificados é a falta de pessoal qualificado para conduzir investigações cibernéticas. A rápida evolução da tecnologia exige que as forças de segurança estejam constantemente atualizadas e bem treinadas para lidar com as novas formas de crimes cibernéticos. A ausência de especialistas em cibersegurança nas instituições policiais e judiciais compromete a capacidade de investigação e resolução desses crimes, resultando em baixos índices de detecção e punição.

Além disso, a demora na atualização legislativa para acompanhar as novas modalidades de crimes cibernéticos é outra barreira significativa. As leis existentes, muitas vezes, não conseguem abarcar todas as nuances e complexidades dos crimes digitais modernos. Por exemplo, o uso de criptomoedas para financiar atividades ilícitas ou a exploração de vulnerabilidades em sistemas de inteligência artificial são áreas que ainda carecem de uma regulamentação específica e eficiente. Essa

defasagem legislativa cria brechas que podem ser exploradas por criminosos, dificultando a aplicação da justiça.

A pesquisa também destacou a importância de uma maior conscientização e preparo dos usuários de tecnologias para prevenir e mitigar os riscos associados aos crimes cibernéticos. Muitos crimes cibernéticos se aproveitam da falta de conhecimento dos usuários sobre práticas seguras na internet. *Phishing*, engenharia social e outras técnicas de manipulação são frequentemente utilizadas para enganar indivíduos e obter acesso a informações confidenciais. Portanto, a promoção de campanhas educativas que visem aumentar a alfabetização digital e a conscientização sobre cibersegurança é crucial para reduzir a vulnerabilidade dos usuários.

Além das campanhas educativas, o treinamento especializado para forças de segurança é essencial. A criação de unidades especializadas em cibercrimes dentro das instituições policiais e judiciais pode melhorar significativamente a capacidade de resposta às ameaças cibernéticas. Essas unidades devem ser equipadas com tecnologias avançadas e contar com profissionais altamente qualificados, capazes de conduzir investigações complexas e identificar padrões de comportamento criminoso na internet.

Outra medida importante é a promoção de parcerias entre o governo, o setor privado e a sociedade civil para fortalecer a segurança cibernética. O combate aos crimes cibernéticos requer um esforço colaborativo e coordenado, envolvendo diversas partes interessadas. As empresas de tecnologia, por exemplo, podem desempenhar um papel fundamental ao desenvolver soluções de segurança inovadoras e compartilhar informações sobre ameaças cibernéticas com as autoridades. A sociedade civil, por sua vez, pode contribuir com iniciativas de conscientização e apoio às vítimas de crimes cibernéticos.

Ademais, a cooperação internacional é vital para enfrentar os crimes cibernéticos, que frequentemente envolvem redes transnacionais de criminosos. A internet não conhece fronteiras, e muitos ataques cibernéticos são orquestrados a partir de diferentes países, tornando essencial a colaboração entre nações para rastrear e punir os responsáveis. O Brasil deve fortalecer suas relações com organismos internacionais e participar ativamente de iniciativas globais de combate ao cibercrime, compartilhando informações e boas práticas.

Os achados da pesquisa também indicaram a necessidade de uma maior integração entre as diferentes esferas do governo para a implementação de políticas eficazes de cibersegurança. A criação de um marco regulatório abrangente, que coordene as ações entre órgãos como a Polícia Federal, o Ministério da Justiça, a Agência Nacional de Telecomunicações (Anatel) e outros, pode garantir uma resposta mais eficiente e coesa às ameaças cibernéticas. A definição de responsabilidades claras e a alocação adequada de recursos são passos fundamentais para fortalecer a estrutura de cibersegurança do país.

Além das medidas preventivas e repressivas, a pesquisa sugere a importância de um sistema judicial capacitado para lidar com os crimes cibernéticos. A formação contínua de juízes e promotores em temas de cibersegurança é crucial para garantir que os processos judiciais sejam conduzidos com o conhecimento técnico necessário. A adoção de tecnologias judiciais que facilitem a gestão de provas digitais e a realização de audiências virtuais também pode contribuir para a eficiência do sistema judicial no tratamento de casos de crimes cibernéticos.

Por fim, a pesquisa apontou a necessidade de um acompanhamento constante das políticas e práticas de cibersegurança, com a realização de estudos periódicos e a avaliação dos resultados obtidos. A criação de um observatório nacional de cibersegurança, que monitore as tendências e desafios emergentes, pode fornecer dados valiosos para a formulação de políticas públicas e a adaptação das estratégias de combate aos crimes cibernéticos.

Em conclusão, os achados desta pesquisa revelam um cenário complexo e desafiador para o combate aos crimes cibernéticos no Brasil. Embora existam avanços significativos na legislação e na conscientização sobre o tema, ainda há muito a ser feito para garantir uma resposta eficaz às ameaças cibernéticas. A formação de pessoal qualificado, a atualização constante das leis, a promoção de parcerias e a cooperação internacional são elementos essenciais para fortalecer a cibersegurança e proteger a sociedade brasileira dos impactos negativos dos crimes cibernéticos.

## 6 CONSIDERAÇÕES FINAIS

A realidade futura exige que a legislação, a doutrina e a jurisprudência brasileiras se adaptem ao crescimento contínuo dos crimes virtuais, à medida que os avanços tecnológicos continuam a introduzir novas inovações.

A legislação atual para tratar de crimes digitais é considerada ineficaz, apesar de sua contínua evolução. Entretanto, a Lei nº 12.737/2012 é um avanço legislativo significativo, pois busca garantir a segurança e salvaguardar o direito à privacidade dos dados e informações das pessoas no âmbito digital.

A ideologia hacker, criada no MIT, tem como objetivo promover o fluxo irrestrito de informações e conhecimentos entre os diversos componentes da sociedade global, para o benefício coletivo da humanidade. Atualmente, a comunidade de hackers defende seis regras, conhecidas como ética dos hackers, para evitar a confusão entre hackers e criminosos cibernéticos (*crackers*) em sua identificação.

A regra pode ser percebida como um impedimento substancial contra indivíduos que se envolvem em *cyberbullying*, em vez de uma medida enganosa ou fraudulenta. No entanto, outra questão é se essa é a penalidade adequada de forma consistente. Em termos práticos, parece que somente os casos com repercussões significativas para as vítimas são capazes de gerar penalidades legais. Portanto, os governos devem combater o *cyberbullying* com base em um entendimento mais amplo. Atualmente, existem amplos recursos legais que tratam de um amplo espectro de comportamentos que podem ser classificados como *bullying*.

As leis civis e criminais tratam de vários casos de comportamento persistente e hostil. Há várias leis que tratam de assédio, intimidação, ameaças, difamação, violação de privacidade e outros tipos de má conduta. É provável que qualquer nova legislação replique ou duplique os recursos legais já existentes. Os formuladores de políticas devem ter cautela para evitar exacerbar a complexidade de um sistema judicial já inacessível.

A autoridade para censurar também representa um perigo tangível e significativo para a liberdade de expressão. Os direitos humanos, incluindo o direito à liberdade de expressão, são de extrema importância, pois garantem a preservação da dignidade humana. Uma abordagem centrada na censura prejudica o desenvolvimento de habilidades cruciais, como a resolução de problemas, a autorregulação e o gerenciamento de riscos, que são essenciais para o bom

funcionamento da sociedade desde a juventude. É obrigação coletiva de cada indivíduo abordar e prevenir ativamente o *cyberbullying*. Há uma ampla gama de ferramentas disponíveis para prestar assistência. A implementação de estratégias eficazes para a navegação na Internet, a otimização do posicionamento de computadores e dispositivos dentro de casa e a utilização de software adequado podem equipar os pais com as ferramentas necessárias para conter a proliferação dessa influência malévola.

## REFERÊNCIAS

BITTAR, Eduardo CB. Internet, **Cyberbullying e Lesão a Direitos da Personalidade**: o alcance atual da teoria da reparação civil por danos morais. Homenagem a José de Oliveira Ascensão. Revista do Instituto do Direito Brasileiro, v. 3, n. 3, p. 1695-1715, 2014.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, nas Redes Sociais**, São Paulo, 2022, p. 3177.

COMER, Douglas. **Interligação de Redes com TCP/IP—**: Princípios, Protocolos e Arquitetura. Elsevier Brasil, 2016.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. Editora Saraiva, 2017.

CUNHA, Rogério Sanches. **Manual de Direito Penal**, 13ª Edição, Salvador, 2021, p. 408.

DIAS, Vilson. **Crimes Virtuais**: Estudo Introdutório, Edição Portuguesa, São Paulo, 2021. p. 7.

DINO. Crimes virtuais afetam 42 milhões de brasileiros, **juritec**. 2019.

DOMINGOS, Vanessa Santiago da Silva *et al.* **O Inefetivo Tratamento do Cyberbullying no Brasil**: a busca de mecanismos eficazes de combate. 2019. Disponível em: <http://ri.ucsal.br:8080/jspui/handle/prefix/546>.

FELICIANO, Guilherme Guimarães. **Informática e Criminalidade**. Parte I: lineamentos e definições. Boletim do Instituto Manoel Pedro Pimentel, São Paulo, v. 13, n. 2, p. 35-45, set. 2000. p. 42.

GILABERTE, Bruno. **Crimes Contra a Pessoa**, 3ª Edição, Rio de Janeiro, 2021.

GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. **Boletim do IBCCrim**. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

JUSBRASIL. **Crimes virtuais: conceito e seus tipos**: Disponível em: <https://carino311.jusbrasil.com.br/artigos/307607071/crimes-virtuais-conceito-e-seus-tipos>

LOPES, Amanda; MONTEIRO, Daniela Fernandes; ROCHA, Cíntia Pavani Motta. **Cyberbullying no Ordenamento Jurídico Brasileiro**. 13ª Mostra de Iniciação Científica, v. 1, 2016. Disponível em: <http://trabalhos.congrega.urcamp.edu.br/index.php/mic/article/view/1117>. Acesso em: ago. /2019.

MOURA, Teles Ney. Direito penal: parte especial. São Paulo: Atlas, v.2, 2004.

NASCIMENTO, Bárbara Luiza Coutinho do. **Liberdade de Expressão, Honra e Privacidade na Internet**, 1ª Edição, Rio de Janeiro, 2010, p. 7

NORONHA, Edgard Magalhães. Código Penal Brasileiro Comentado. 2. Ed. São Paulo: Saraiva, 1958. V 5, 1ª e 2ª partes.

PIAIA, Thami Covatti; RITTER, Letícia Mousquer; SANGOI, Rafael Martins. **Liberdade de Expressão Publicada Versus Anonimato**: a (ir) responsabilização no cyberbullying. Revista Eletrônica Direito e Política, v. 13, n. 2, p. 1016-1047, 2018.

ROQUE, Sérgio Marcos. **Criminalidade Informática**: crimes e criminosos do computador. São Paulo: ADPESP Cultural, 2007. P. 25.

ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal**. São Paulo: Memória Jurídica, 2004, P. 123.

SCHMIDT, Guilherme. **Crimes Cibernéticos:** Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos> 2014.

\_\_\_\_\_, Guilherme Afonso et al. **O Fenômeno do Cyberbullying**. DI@ LOGUS, v. 4, n. 2, p. 127-134, 2015.

SCHREIBER, Fernando Cesar de Castro; ANTUNES, Maria Cristina. **Cyberbullying: do Virtual ao Psicológico**. Boletim-Academia Paulista de Psicologia, v. 35, n. 88, p. 109-125, 2015. Disponível em: [http://pepsic.bvsalud.org/scielo.php?pid=S1415-711X2015000100008&script=sci\\_abstract&lng=es](http://pepsic.bvsalud.org/scielo.php?pid=S1415-711X2015000100008&script=sci_abstract&lng=es). .

SILVA, Ângelo Roberto Ilha da. **Crimes Cibernéticos** - 2ª Ed. Porto Alegre: Liv. do Advogado Ed., 2017.

VANCIM, Adriano Roberto; GONÇALVES, José Eduardo Junqueira. **Os Cybers Crimes e o Cyberbullying:** apontamentos jurídicos ao direito da intimidade e da privacidade. Em: Jurisprudência mineira, Belo Horizonte: Tribunal de Justiça de Minas Gerais, v. 62, n. 199, out/dez. 2011, p. 36-43, 2011.

VECTRA, Consultoria e serviços. **Conheça os 6 Principais Tipos de Crime na Internet** Disponível em: <https://blog.vectras.com.br/conheca-os-6-principais-tipos-de-crime-na-internet/>.