CENTRO UNIVERSITÁRIO PARA O DESENVOLVIMENTO DO ALTO VALE DO ITAJAÍ – UNIDAVI

WELLINGTON DA SILVA

OS MECANISMOS DE INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

PRESIDENTE GETÚLIO

2023

CENTRO UNIVERSITÁRIO PARA O DESENVOLVIMENTO DO ALTO VALE DO ITAJAÍ – UNIDAVI

WELLINGTON DA SILVA

OS MECANISMOS DE INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito, pelo Centro Universitário para o Desenvolvimento do Alto Vale do Itajaí - UNIDAVI

Orientador: Prof. Esp. Nilton Martinez Loureiro Filho

PRESIDENTE GETÚLIO

2023

CENTRO UNIVERSITÁRIO PARA O DESENVOLVIMENTO DO ALTO VALE DO ITAJAÍ – UNIDAVI

A monografia intitulada **"OS MECANISMOS DE INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS"**, elaborada pelo acadêmico WELLINGTON DA SILVA, foi considerada

( ) APROVADA

( ) REPROVADA

por todos os membros da banca examinadora para a obtenção do título de BACHAREL EM DIREITO, merecendo nota _____.

_____, _____ de _____ de _____.

_____

Profa. M.ª Vanessa Cristina Bauer

Coordenadora do Curso de Direito

Apresentação realizada na presença dos seguintes membros da banca:

Presidente: _____

Membro: _____

Membro: _____

TERMO DE ISENÇÃO DE RESPONSABILIDADE

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico conferido ao presente trabalho, isentando o Centro Universitário para o Desenvolvimento do Alto Vale do Itajaí, a Coordenação do Curso de Direito, a Banca Examinadora e o Orientador de toda e qualquer responsabilidade acerca do mesmo.

Presidente Getúlio, 04 de novembro de 2023.

Wellington Da Silva
Acadêmico

Dedico este trabalho à minha esposa e aos meus pais.

RESUMO

O presente Trabalho de Conclusão de Curso tem como objetivo analisar os mecanismos de investigação dos crimes cibernéticos, para tanto, dissertou-se sobre o uso da internet como meio para o cometimento de crimes, trazendo o conceito, surgimento e espécies de crimes cibernéticos. Em seguida, buscou-se apresentar os principais crimes cibernéticos previstos no ordenamento jurídico brasileiro, quais sejam: o estupro virtual, a pornografia de vingança, o estelionato virtual, o furto qualificado por meio informático, a calunia, injúria, difamação e a invasão de dispositivos. Por fim, foi explorado os mecanismos de investigação de crimes cibernéticos, onde buscou-se apresentar os meios investigatórios na legislação vigente, de acordo com a Lei Carolina Dieckmann, o Marco Civil da Internet e o Código de Processo Penal, para então adentrar nas questões relacionadas à perícia computacional e as dificuldades de investigação e repressão dos crimes cibernéticos. O método de abordagem utilizado na elaboração desse trabalho de curso foi o indutivo; o método de procedimento foi o monográfico e o levantamento de dados ocorreu através da técnica da pesquisa bibliográfica. O ramo de estudo foi na área do Direito Penal e Direito Processual Penal. Nas considerações finais, trabalhou-se com as partes principais do tema, bem como a comprovação da hipótese básica elencada na introdução do presente trabalho, de que o ordenamento jurídico brasileiro não possui mecanismos de investigação suficientes para investigar e combater os crimes cibernéticos.

Palavras-chave: crimes cibernéticos; investigação; mecanismos.

ABSTRACT

The present Course Completion Work aims to analyze the mechanisms of cybercrime investigation. To do so, it delves into the use of the internet as a means for committing crimes, presenting the concept, emergence, and types of cybercrimes. Subsequently, it seeks to outline the main cybercrimes specified in Brazilian law, namely: virtual rape, revenge porn, virtual fraud, qualified theft by computer means, slander, insult, defamation, and device intrusion. Finally, the work explores mechanisms for investigating cybercrimes, aiming to present investigative methods within current legislation in accordance with the Carolina Dieckmann Law, the Brazilian Civil Rights Framework for the Internet, and the Code of Criminal Procedure. It also delves into issues related to digital forensics and the challenges of investigating and suppressing cybercrimes. The approach method used in this coursework was inductive, the procedure method was monographic, and data collection was accomplished through bibliographic research techniques. This study falls within the field of Criminal Law and Criminal Procedure. In the concluding remarks, the main aspects of the topic are discussed, as well as the verification of the basic hypothesis outlined in the introduction of this work, that the Brazilian legal system lacks sufficient investigative mechanisms to address and combat cybercrimes.

Keywords: cybercrimes; investigation; mechanisms.

SUMÁRIO

1 INTRODUÇÃO

O objeto do presente Trabalho de Curso são os mecanismos de investigação dos crimes cibernéticos.

O seu objetivo institucional é a produção do Trabalho de Curso como requisito parcial à obtenção do grau de Bacharel em Direito pelo Centro Universitário para o Desenvolvimento do Alto Vale do Itajaí – UNIDAVI.

O objetivo geral deste trabalho de curso é analisar os mecanismos de investigação dos crimes cibernéticos.

Os objetivos específicos são: a) comentar sobre o uso da internet como meio para o cometimento de crimes; b) discutir os crimes cibernéticos previstos no ordenamento jurídico brasileiro; c) analisar os mecanismos de investigação dos crimes cibernéticos.

Na delimitação do tema levanta-se o seguinte problema: o ordenamento jurídico brasileiro possui mecanismos de investigação suficientes para investigar e combater os crimes cibernéticos?

Para o equacionamento do problema levanta-se a seguinte hipótese: supõe-se que o ordenamento jurídico brasileiro não possui mecanismos de investigação suficientes para investigar e combater os crimes cibernéticos.

O método de abordagem a ser utilizado na elaboração desse trabalho de curso será o indutivo; o método de procedimento será o monográfico. O levantamento de dados será feito através da técnica da pesquisa bibliográfica.

A justificativa do tema em questão se baseia na medida em que o progresso da tecnologia trouxe inúmeros vantagens, incluindo o acesso à informação e a capacidade de comunicação através da internet com pessoas que estão geograficamente distantes. No entanto, ele também desempenhou um papel na origem de novos delitos e na simplificação da prática de crimes que já existiam no mundo real e agora são cometidos no espaço virtual.

A rápida evolução tecnológica tem gerado desafios significativos para o campo jurídico. Essas mudanças levantam questões sobre como equilibrar a liberdade de expressão com a proteção de direitos fundamentais, como dignidade, intimidade, honra e imagem, que podem ser afetados pela utilização desenfreada da tecnologia. A internet, sendo utilizada por pessoas de diferentes países, muitas vezes parece um lugar sem leis, permitindo a ocorrência virtual de crimes.

O principal desafio é acompanhar e compreender essas inovações para assegurar a paz social, o desenvolvimento das relações modernas e a manutenção do Estado Democrático de Direito. Isso exige que os profissionais do direito encontrem maneiras de lidar com as novas questões que surgem neste novo paradigma. Portanto, é crucial buscar uma regulamentação legal que garanta a eficácia e a segurança das relações em um ambiente virtual, considerando a realidade da internet, as relações em constante evolução e a globalização que ela permite.

As inovações tecnológicas também requerem alterações nas leis para abordar novas situações e objetivos sociais, mantendo a liberdade individual e os princípios do Estado de Direito, promovendo o funcionamento da ordem democrática e estimulando o desenvolvimento econômico e tecnológico.

O combate a crimes relacionados à tecnologia exige profissionais altamente especializados, equipados com ferramentas específicas para lidar com provedores de acesso, conteúdo, instituições bancárias e representantes de redes sociais. Para efetivamente enfrentar essa forma de criminalidade, é fundamental que o Estado invista mais em recursos e desenvolvimento na área de investigação, incluindo a especialização de agentes e a aquisição de equipamentos de informática avançados. Isso é essencial para garantir uma prestação jurisdicional eficaz à sociedade.

Para isso, principia-se, no Capítulo 2 dissertar sobre o uso da internet como meio para o cometimento de crimes, onde será abordado o conceito, o surgimento e as espécies de crimes cibernéticos, que se dividem em impróprios e próprios.

O Capítulo 2 trata dos crimes cibernéticos previstos no ordenamento jurídico brasileiro, onde será analisado o estupro virtual, a pornografia de vingança, o estelionato virtual, o furto qualificado por meio informático, a calúnia, injúria, difamação e a invasão de dispositivos.

O Capítulo 3 dedica-se a analisar os mecanismos de investigação de crimes cibernéticos, observando os meios investigatórios na legislação vigente, conforme a Lei Carolina Dieckmann, o Marco Civil da Internet e o Código de Processo Penal, para então adentrar nas questões envolvendo a perícia computacional e as dificuldades de investigação e repressão dos crimes cibernéticos.

O presente Trabalho de Curso encerrar-se-á com as Considerações Finais nas quais serão apresentados pontos essenciais destacados dos estudos e das reflexões realizados sobre os mecanismos de investigação dos crimes cibernéticos.

2 O USO DA INTERNET COMO MEIO PARA O COMETIMENTO DE CRIMES

A rápida transformação que a sociedade passou com o uso da tecnologia, trouxe diversas problemáticas a serem enfrentadas pelas ciências jurídicas, em busca de solução aos novos problemas que a ferramenta pode apresentar nas relações sociais, principalmente em razão da utilização desenfreada, que pode se chocar com direitos fundamentais como à dignidade, à intimidade, à honra e à imagem, que também devem ser respeitados, em face ao direito à liberdade de expressão.[1]

Essa utilização da internet por usuários dos mais variados países, traz uma sensação de ser uma terra sem lei, fazendo com que alguns crimes começaram a ser introduzidos virtualmente.[2] O grande desafio é compreender e acompanhar as inovações para garantir a pacificação social, o desenvolvimento das novas relações e a manutenção do Estado Democrático de Direito, cabendo aos operadores do direito encontrar meios para responder às novas demandas que se originarem do novo paradigma. Assim, considerando a realidade virtual, as novas relações que se consolidam a cada instante e a globalização que a internet permite, é importante buscar uma tutela jurídica capaz de garantir a efetividade e segurança para estas relações.[3]

As inovações tecnológicas provocam alterações nas legislações na medida em que se espera meios adequados para lidar com as novas situações e otimizar os novos objetivos da ordem jurídica e social, com a manutenção da liberdade individual e dos princípios do Estado de Direito, o funcionamento da ordem democrática, bem como, a promoção do desenvolvimento econômico e tecnológico.[4]

Apesar de inúmeros benefícios e facilidades para a sociedade, a internet também colaborou para o surgimento de uma série de crimes praticados em ambientes virtuais ou com a facilitação desses, fazendo com que o legislador brasileiro

---

[1] MARTINI, Kelly de; LACERDA, Emanuela Cristina Andrade. O direito, a informática e a sociedade. **Revista do Curso de Direito da FSG**, ano 6, n. 11, jan./jun. 2012, p. 53-61. Disponível em: https://ojs.fsg.edu.br/index.php/direito/article/view/346/320. Acesso em: 28 jun. 2023.

[2] COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

[3] FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital e a sociedade da informação.** 2. ed. São Paulo: Saraiva, 2016. p. 17.

[4] HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital:** transformação digital: desafios para o direito. 2. ed. Rio de Janeiro: Forense, 2022. p. 31.

se preocupasse em tipificar novas condutas e abranger as já existentes.[5] Isso porque, o Código Penal e as legislações penais especiais foram afetadas por esta nova realidade, uma vez que a internet é uma ferramenta global que interfere nas tradicionais regras de aplicação da lei penal no espaço.[6]

Os delitos que ocorrem na rede mundial de computadores, trazem uma sensação de anonimidade, de modo que o autor age com a ideia de que não pode ser percebido, ao passo que a vítima tem a sensação de segurança, pois não visualiza os riscos de forma clara.[7] Tais delitos tomaram grandes proporções com a sociedade digital e apresentam grandes desafios para o seu combate, pois há dificuldade em localizar a identidade dos autores e o desenvolvimento da respectiva persecução penal, surgindo um novo modelo jurídico que necessita lidar de forma adequada em investigações que envolvam recursos tecnológicos para a prática criminosa.[8]

Nesse sentido, destacam Alexandre Rocha Almeida de Moraes, Isabella Tucci Silva e Bruno Santiago: “a globalização, antes imaginada para fins econômicos, tornou-se cultural e, como todas as grandes revoluções da humanidade, trouxe benefícios e ônus como a criminalidade cibernética“.[9]

Assim, o uso da internet como meio para o cometimento de crimes é um fenômeno que tem crescido significativamente nas últimas décadas, à medida que a tecnologia e a conectividade online se tornaram partes integrantes da vida cotidiana. Sob esse contexto, este capítulo irá abordar os principais aspectos relacionados ao

---

[5]MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Borges. Os crimes cibernéticos no ordenamento jurídico brasileiro e a necessidade de legislação específica. **GPC ADVOGADOS.** Disponível em: http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-ea-necessidade-de-legislacao-especifica-2. Acesso: 23 out. 2023.

[6] TOMASEVICIUS FILHO, Eduardo. Marco civil da internet: uma lei sem conteúdo normativo. **Estudos Avançados,** Atualidades. v. 30 (86). Jan-Apr 2016. Disponível em: https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/. Acesso em: 28 jun. 2023.

[7] SYDOW, Spencer Toth. **Delitos informáticos próprios:** uma abordagem sob a perspectiva vitimodogmática. Dissertação para o Departamento de Direito Penal, Medicina Forense e Criminologia. Universidade de São Paulo, 2009. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-15062011-161113/publico/Dissertacao_Mestrado_versao_final_formatada_padroes_US.pdf. Acesso em: 28 jun. 2023. p. 32.

[8] BRASIL. **Crimes cibernéticos.** Brasília: Ministério Público Federal, 2018. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 28 jun. 2023. p.10.

[9] MORAES, Alexandre Rocha Almeida de; SILVA, Isabella Tucci; SANTIAGO, Bruno. Os cibercrimes e a investigação digital: novos paradigmas para a persecução penal. **Momentum**, Atibaia, v. 1, n. 18, p. 1-34, 2020. Disponível em: https://momentum.emnuvens.com.br/momentum/article/download/284/201/557. Acesso em: 04 set. 2023.

uso da internet como meio para o cometimento de crimes, descrevendo, em suma, o conceito de crime cibernético, o surgimento dos primeiros crimes cibernéticos e suas espécies.

2.1 CONCEITO DE CRIME CIBERNÉTICO

Crime cibernético é conceituado como o fato típico e antijurídico, que é cometido através da informática ou contra o sistema informático, sendo este o bem ofendido ou o meio para praticar ofensa a bens protegidos pelo ordenamento jurídico brasileiro.[10]

Sérgio Marcos Roque traz em sua definição, como sendo: “toda conduta, definida em lei como crime, em que o computador tenha sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material”.[11] Patrícia Peck Pinheiro leciona:

> O crime eletrônico é, em princípio, um crime de meio, isto é, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por hackers, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isso quer dizer que o meio de materialização da conduta criminosa pode ser virtual; contudo, em certos casos, o crime não. A maioria dos crimes cometidos na rede facilitador, principalmente pelo anonimato que proporciona.
> Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital. As principais inovações jurídicas trazidas no âmbito digital se referem à territorialidade e à investigação probatória, bem como à necessidade de tipificação penal de algumas modalidades que, em razão de suas peculiaridades, merecem ter um tipo penal próprio.[12]

Para Emerson Wendt e Higor Vinicius Nogueira Jorge:

> Os crimes virtuais são todas as condutas típicas, antijurídicas e culpáveis praticadas com a utilização de computadores ou qualquer outro sistema de informática, sendo estes diversos e tendo como classificação mais aceita a distinção entre crimes cibernéticos puros/próprios ou impuros/impróprios, tendo o autor do crime como o agente ativo, popularmente conhecido como

[10] JESUS, Damásio de; OLIVEIRA, José Antonio Milagre de. **Manual de crimes informáticos.** 1. ed. São Paulo: Saraiva, 2016. p. 49.
[11] ROQUE, Sérgio Marcos. **Criminalidade Informática:** crimes e criminosos do computador. 1. ed. São Paulo: ADPESP Cultural, 2007. p. 25.
[12] PINHEIRO, Patrícia Peck. **Direito digital.** 7. ed. São Paulo: Saraiva, 2021. p. 164.

> hacker ou cracker, e qualquer pessoa física ou jurídica ou uma entidade titular, pública ou privada, que sofra a ação ou sobre quem recaiu tal ação é o agente passivo do crime.[13]

Para Carla Rodrigues Araújo Castro: “crime de informática é aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através de computador”.[14] O crime cibernético não utiliza do contato físico entre o agente e a vítima, podendo ocorrer em ambientes sem pessoas, governo ou território, além de não gerar sensação de violência, em comparação com os delitos de ordem física.[15]

Desta forma, percebe-se que trata-se de ilícitos consumados através da internet ou com o auxílio desta, trazendo algum dano à vítima ou à coletividade, podendo ainda ser praticado contra o próprio sistema de informática.[16]

2.2 SURGIMENTO DOS CRIMES CIBERNÉTICOS

Como visto, os delitos praticados contra ou por meio do sistema informático são denominados de crimes cibernéticos, termo utilizado para definir as condutas realizadas através da internet e que causam certo dano à vítima, os quais podem se concretizar através da internet ou praticados contra o sistema informático, visando causar dano a este.[17] Assim, embora a internet tenha trazido diversos benefícios para a população, também trouxe aspectos negativos, como a criação de novos crimes e a adaptação dos crimes já existentes ao ambiente virtual pelos agentes. Nesse sentido, Mário Furlaneto Neto e José Augusto Chaves Guimarães destacam:

---

[13] WENDT, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos:** ameaças e procedimentos de investigação. 1. ed. São Paulo: Editora Brasport, 2012. p. 65.

[14] CASTRO, Carla Rodrigues Araújo. **Crimes de informática e seus aspectos processuais.** 2. ed. Rio de Janeiro: Lumen Juris, 2001. p. 9.

[15] SYDOW, Spencer Toth. **Delitos informáticos próprios:** uma abordagem sob a perspectiva vitimodogmática. Dissertação para o Departamento de Direito Penal, Medicina Forense e Criminologia. Universidade de São Paulo, 2009. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-15062011-161113/publico/Dissertacao_Mestrado_versao_final_formatada_padroes_US.pdf. Acesso em: 28 jun. 2023.p. 46.

[16] FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital e a sociedade da informação.** 2. ed. São Paulo: Saraiva, 2016. p. 39.

[17] WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos:** ameaças e procedimentos de investigação. 1. ed. São Paulo: Editora Brasport, 2012. p. 36.

> [...] os transgressores da lei penal logo viram no computador e na Internet formidáveis instrumentos à consecução de vários delitos. Como se não bastasse, essa revolução tecnológica também deu azo à criatividade delituosa, gerando comportamentos inéditos que, não obstante o alto grau de reprovabilidade social, ainda permanecem atípicos [18]

Jaqueline Ana Buffon aponta que atualmente a internet é um dos meios mais comuns para a prática de crimes em razão das características que resultam em dificuldade investigativa, motivando os agentes a utilizarem esse novo meio para executar seus objetivos, dessa forma ela destaca as principais características:

> a. anonimato – o uso sofisticado do ciberespaço e das Tecnologias de Informação e Comunicação (TICs) muitas vezes possibilita um anonimato que resulta em maiores dificuldades de investigação, especialmente quando se utilizam da Dark Web, por meio da ferramenta The Onion Router ou outras.
> b. âmbito geográfico – necessidade de uma eficaz cooperação internacional para se obter êxito nas investigações, considerando a diversidade de locais entre a execução da ação ilícita e (o)s resultado(s), além da utilização de servidores em locais que podem ser considerados “paraísos virtuais”;
> c. custo/benefício do meio empregado – a comunicação imediata que o meio proporciona, não existindo fronteiras físicas para a execução. O alcance e a propagação ocorrem num tempo extraordinário por um custo mínimo.[19]

Os primeiros casos de crimes virtuais ocorreram em 1960, com a manipulação e sabotagem de sistemas de computadores.[20] Entretanto, somente na década de 70 os sujeitos ativos dessas infrações ficaram conhecidos, sendo denominados de *hackers*. Em 1980 a prática dos delitos informáticos se expandiu, onde os *hackers* passaram a subtrair, modificar e destruir dados que estavam presente nos ambientes virtuais, passando então a praticar crimes que já estavam presente na sociedade, mas através da internet, facilitando sua propagação.[21]

---

[18] FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. Crimes Na Internet: elementos para uma reflexão sobre a ética informacional - **R. CEJ**, Brasília, n. 20, p. 67-73, jan./mar. 2003 Disponível em: https://revistacej.cjf.jus.br/cej/index.php/revcej/article/view/523. Acesso em: 23 out. 2023.

[19] BUFFON, Jaqueline Ana. Agente infiltrado virtual. In: BRASIL. **Crimes cibernéticos.** 2ª Câmara de Coordenação e Revisão, Criminal. Ministério Público Federal. Brasília: MPF, 2018. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 25 out. 2023. p. 76.

[20]CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. **Âmbito Jurídico.** Disponível em http://www.ambitojuridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17. Acesso em: 28 jun. 2023.

[21] ANDRADE, Mariah Dourado de; BENTES, Dorinethe dos Santos; GUIMARAES, David Franklin da Silva. Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais. **Revista Vertentes do Direito.** Disponível em: https://redib.org/Record/oai_articulo1568032-considera%C3%A7%C3%B5es-sobre-a-aplicabilidade-do-direito-penal-acerca-dos-crimes-virtuais. Acesso em: 28 jun. 2023.

Os primeiros vírus eletrônicos que há relato surgiram na década de 80, sendo um desenvolvido em 1982 por Elk Cloner que era capaz de contaminar computadores da marca *Apple* e se difundia por cópias de disquetes contaminados. Posteriormente, em 1984, outro vírus foi desenvolvido por um grupo de programadores que criaram um jogo chamado *Core Wars* que era capaz de se reproduzir e cada vez que era executado sobrecarregava a memória do computador do jogador. Os mesmos desenvolvedores criaram um programa antivírus capaz de destruir as cópias geradas pelo jogo em questão.[22]

No ano de 1986 dois irmãos paquistaneses desenvolveram um vírus chamado de *Brain*, que atingia o setor de inicialização do disco rígido do computador que detectava o uso não autorizado de um *software* médico de monitoramento cardíaco que havia sido desenvolvido na época. No entanto, o código acabou sofrendo algumas alterações maliciosas, transformando o vírus que se espalhava por disquetes infectados, causando lentidão nos sistemas de operações do sistema e ocupando a memória ocupacional dos computadores.[23]

No mesmo ano surgiu o primeiro Cavalo de Tróia, conhecido como PC Write, que se apresentava como um editor de texto que quando executado, corrompia os arquivos do disco rígido do computador, sendo responsável por invadir computadores e acessar informações de todos os dados que estavam arquivados na memória do computador, além de infectar outros dispositivos que estivessem conectados.[24]

Em 1990, um grupo das nações do G8 se reuniu em Lyon, na França, para debater sobre os graves crimes que vinham ocorrendo por dispositivos eletrônicos conectados à internet ou contra estes dispositivos, onde surgiu o termo cibercrime, utilizado para informar os crimes cometidos pela internet.[25] Com isso, os agentes conseguiam obter acesso aos computadores das vítimas, independentemente do local

---

[22]WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos:** ameaças e procedimentos de investigação. 1. ed. São Paulo: Editora Brasport, 2012.

[23]D'URSO, Filizzola Luiz. Em Tempos de Cibercrimes. **Migalhas,** 2019. Disponível em: https://www.migalhas.com.br/dePeso/16,MI310551,31047-Em+tempos+de+cibercrimes. Acesso em: 28 jun. 2023.

[24]MONTEIRO, Neto. **Aspectos constitucionais e legais do crime eletrônico.** Dissertação de Pós-Graduação em Direito. Universidade de Fortaleza, 2008. Disponível em: https://bdtd.ibict.br/vufind/Record/UFOR_35c4cc8a1b88754a2fbdd093192cf6dc. Acesso em: 28 jun. 2023.

[25]NASCIMENTO, Samir de Paula. Cibercrime: conceitos, modalidades e aspectos jurídicos-penais. **Âmbito Jurídico.** Disponível em: https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitosmodalidades-e-aspectos-juridicos-penais/. Acesso em: 28 jun. 2023.

geográfico e do controle, principalmente através da disseminação de vírus intencionalmente desenvolvidos com a intenção de causar um dano específico.[26]

No início do século XXI os crimes cibernéticos passaram a ser mais frequentes e a internet, por ser um ambiente virtual de dimensão incalculável, proporciona diversas formas para a consumação de delitos. Dentre as principais formas de ataque e contaminação no sistema informático estão os vírus, os *trojans* e os *worms.*[27]

Os vírus são programas escritos em linguagem de programação, que contaminam outros programas do computador por meio de sua modificação, incluindo uma cópia de si mesmo. Já os *trojans*, mais conhecidos como cavalos de tróia ou *backdoors,* são programas enviados à um sistema anfitrião que permite a conexão do computador infectado com o computador do invasor, sem a necessidade de autorização, o que permite que o invasor controle e monitore as atividades do usuário.[28] Importante fazer um liame entre as formas de contaminação nos computadores com a noção que os usuários possuem quando utilizam a rede, conforme descreve Spencer Toth Sydow:

> O cidadão virtual comum transita pelas cibervias deparando-se constantemente com outros cidadãos e, por não haver identidade, aparência ou limites sociais, não consegue identificar o bem do mal intencionado. Todos são idênticos na rede e há que se aceitar que por mais delinquentes que haja no mundo real, estes são exceções sociais, prevalecendo o homem de bem que não traz prejuízos ao próximo. Destarte, navega-se na rede partindo-se do mesmo pressuposto: a maioria dos contatos e relacionamentos virtuais é com pessoas de bem, sem intenções prejudiciais e somado a isso está a ideia de que as pessoas acreditam naquilo que preferem que seja verdade. [29]

Os autores desses delitos não podem ser facilmente vistos e ouvidos, pois geralmente estão ocultos no território virtual, podendo atingir outros países, onde há

---

[26]SOUZA, Henry Leones de; VOLPE, Luiz Fernando Cassilhas. Da ausência de legislação específica para os crimes virtuais. **Revista Eletrônica da Faculdade de Direito de Alta Floresta,** v. 8, n. 2, 2015. Disponível em: https://egov.ufsc.br/portal/conteudo/da-aus%C3%AAncia-de-legisla%C3%A7%C3%A3o-espec%C3%ADfica-para-os-crimes-virtuais. Acesso em: 28 jun. 2023.

[27] TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico.** 6. ed. São Paulo: SaraivaJur, 2022. p. 233.

[28] TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico.** 6. ed. São Paulo: SaraivaJur, 2022. p. 233.

[29] SYDOW, Spencer Toth. **Delitos informáticos próprios:** uma abordagem sob a perspectiva vitimodogmática. Dissertação para o Departamento de Direito Penal, Medicina Forense e Criminologia. Universidade de São Paulo, 2009. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-15062011-161113/publico/Dissertacao_Mestrado_versao_final_formatada_padroes_US.pdf. Acesso em: 28 jun. 2023. p. 38.

distinta legislação. Nesse contexto, denota-se que a evolução da tecnologia faz parte da atual sociedade e traz diversos benefícios para as atuais relações, no entanto, existem sujeitos que aproveitam da vulnerabilidade dos dados e usuários para cometerem delitos de cunho patrimonial e que atingem a privacidade de outrem. [30]

> Com a utilização de vírus, o criminoso conseguia obter acesso ao computador de suas vítimas. O advento da internet e a sua forma de concepção, que permite interconectar equipamentos ao arrepio da distância geográfica e do controle, aliado à facilidade de troca de informações entre usuários que nunca se viram, e provavelmente, nunca se verão, criou uma propícia para o estabelecimento de uma outra classe de programas com objetivos voltados para causar danos a terceiros. Um destes tipos de programas de computador é o chamado vírus. Vírus, então, nada mais são do que programas de computador intencionalmente desenvolvidos, em geral, com intenções maliciosas, de causar dano a um grupo específico de computadores ou à rede em geral.[31]

Além dos delitos praticados por meio dessas invasões, os meios digitais potencializaram o plágio e a contrafação, colocando em risco a propriedade intelectual e os direitos autorais.[32] Acerca da evolução tecnológica e dos delitos cibernéticos, Jésus-María Silva Sánchez descreve:

> O progresso técnico dá lugar, no âmbito da delinquência clássica tradicional (a cometida com dolo direto e de primeiro grau), a adoção de novas técnicas como instrumento que lhe permite produzir resultados especialmente lesivos; assim mesmo, surgem modalidades delitivas dolosas de novo cunho que se projetam sobre espaços abertos pela tecnologia. A criminalidade, associada aos meios informativos e à internet (a chamada ciberdelinquência), é, em seguramente, o maior exemplo de tal evolução. Nessa medida, acresce-se inegavelmente a vinculação do progresso técnico e o desenvolvimento das formas de criminalidade organizada, que operam internacionalmente e constituem claramente novos riscos para os indivíduos e os Estados.[33]

Esse novo cenário é considerado mais complexo, pois dificulta a imputação de responsabilidade pelas ocorrências de fatos delituosos, uma vez que são praticados

---

[30] LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** 2. ed. São Paulo: Atlas, 2011. p. 7.

[31] SOUZA, Henry Leones de; VOLPE, Luiz Fernando Cassilhas. Da ausência de legislação específica para os crimes virtuais. **Revista Eletrônica da Faculdade de Direito de Alta Floresta,** v. 8, n. 2, 2015. Disponível em: https://egov.ufsc.br/portal/conteudo/da-aus%C3%AAncia-de-legisla%C3%A7%C3%A3o-espec%C3%ADfica-para-os-crimes-virtuais. Acesso em: 28 jun. 2023.

[32] TOMASEVICIUS FILHO, Eduardo. Marco civil da internet: uma lei sem conteúdo normativo. **Estudos Avançados,** Atualidades. v. 30 (86). Jan-Apr 2016. Disponível em: https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/. Acesso em: 28 jun. 2023.

[33] SÁNCHEZ, Jésus-Maria Silva. **A expansão do direito penal:** aspectos da política criminal na sociedade pós-industrial. Traduzido por Luiz Otávio de Oliveira Rocha. São Paulo: Editora Revista dos Tribunais, 2002. p. 29.

com auxílio tecnológico que pode garantir o anonimato e impossibilitar a localização dos autores.[34] Assim destacam Maria Eugênia Gonçalves Mendes e Natália Borges Vieira:

> [...] apesar das facilidades e benefícios oferecidos pela internet, esse cenário também é propício para a prática de crimes. Cada vez mais, os criminosos se valem desse meio para praticar os mais variados tipos de crime. Pois, com o advento da internet, os crimes já tipificados pelo Código Penal passaram a ser praticados também no meio virtual, assim como, surgiram novas modalidades de crimes que passaram a ser praticados nesse meio.[35]

Por essa razão, é importante que sejam disponibilizados meios de investigação mais atualizados, bem como, legislações condizentes com a atual realidade tecnológica. No âmbito do direito penal e direito processual penal, a nova realidade jurídica no meio virtual, necessita de mais regulamentações para combater os pontos negativos que a internet acaba por proporcionar, que por vezes facilita o cometimento de crimes e impunidades, em razão da falta de regulamentação.[36]

2.3 ESPÉCIES DE CRIMES CIBERNÉTICOS

A doutrina tem por costume classificar os crimes previstos no Código Penal e os meios utilizados para o crime, os danos provocados, a natureza e as motivações, de forma que na área do crime cibernético não seria diferente, sendo estes classificados em crimes impróprios e próprios[37], conforme será conceituado e diferenciado em seguida.

---

[34] TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico.** 6. ed. São Paulo: SaraivaJur, 2022. p. 233.

[35] MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Borges. Os Crimes Cibernéticos no Ordenamento Jurídico Brasileiro e a Necessidade de Legislação Específica. **GCP ADVOGADOS.** Disponível em: http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-ea-necessidade-de-legislacao-especifica-2. Acesso em: 23 out. 2023.

[36] COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

[37] COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

2.3.1 Crimes cibernéticos impróprios

Por sua vez, o crime cibernético comum é aquele em que o agente utiliza o sistema de informática como mera ferramenta, mas está não é essencial para a execução e consumação do delito.[38] Neste caso, os delitos já ocorriam antes da popularização dos computadores e da internet, mas estes atuam como um meio facilitador ou meio de comunicação entre os agentes.[39]

Conforme lecionam Damásio de Jesus e Vladimir Aras:

> [...] Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço 'real', ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.[40]

São condutas comuns, típicas, antijurídicas e culpáveis, praticadas através de mecanismos informáticos como ferramenta, mas que poderiam ter sido praticadas por outros meios diversos, fora da esfera virtual, como são os casos dos crimes contra a honra.[41]

> No caso de crime impróprio, pode ser perceptível na situação de um crime de homicídio, quando através de dados de informações sobre medicação, um agente de forma ilícita acessa uma rede de informática de determinado estabelecimento hospitalar, induzindo os profissionais de saúde a medicar o paciente com uma dosagem elevada, levando o mesmo ao óbito. Exemplificando um tipo de conduta que acarretaria a classificação para crimes próprios, seria o cometimento do crime que traz o art.313-B, incluído no Código Penal pela lei n° 9.983/03, como segue: Art.313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: pena- detenção, de 3 (três) meses a 2(dois) anos, e multa.
> O artigo em epígrafe retrata a sociedade atual, que tem como direito receber do poder estatal um amparo quanto a segurança jurídica em razão dos crimes inovadores, através das redes de informática, atentando-se para as

---

[38] TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico.** 6. ed. São Paulo: SaraivaJur, 2022. p. 224.

[39] VIEIRA, Tatiana Malta. A convenção de Budapeste sobre crimes cibernéticos e o ordenamento jurídico nacional. **Revista de Direito de Informática e Telecomunicações.** v. 4, p. 197-232. Belo Horizonte, jan. 2009. p. 200.

[40] JESUS, Damásio de. ARAS, Vladmir. Crimes de informática: Uma nova criminalidade. **JUS.** Disponível em: https://jus.com.br/artigos/2250/crimes-de-informatica. Acesso em: 23 out. 2023.

[41] SYDOW, Spencer Toth. **Delitos informáticos próprios:** uma abordagem sob a perspectiva vitimodogmática. Dissertação para o Departamento de Direito Penal, Medicina Forense e Criminologia. Universidade de São Paulo, 2009. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-15062011-161113/publico/Dissertacao_Mestrado_versao_final_formatada_padroes_US.pdf. Acesso em: 28 jun. 2023. p. 46.

> transformações sociais, que elevam os campos para cometimentos de delitos. Portanto, o Legislativo vem buscando soluções quanto as punições e investigações do crime cibernético, sendo o artigo mencionado, uma inovação feita através da lei ora citada.[42]

Como visto, muitos crimes podem ocorrer através da internet, como é o caso do furto, estelionato, calúnia, entre outros, que utilizam o sistema informático como meio para a execução e consumação do delito. Desse modo, o próximo capítulo se ocupa em abordar o crime de estelionato eletrônico de acordo com a alteração promovida pela Lei n° 14.155/2021, realizando um breve comentário dos aspectos históricos sobre o crime de estelionato, para então adentrar especificamente a sua modalidade eletrônica.

2.3.2 Crimes cibernéticos próprios

São nomeados, como crimes cibernéticos puros, aqueles que ocorrem quando o sujeito visa especialmente atingir o sistema de informática, seja por atos contra o computador e seus componentes ou contra dados e programas digitais, como por exemplo em ações que se materializam por atos contra a integridade do sistema ou acesso desautorizado ao computador.[43] Trata-se do delito praticado por meio de um computador que se consuma também em ambiente eletrônico, onde o sujeito ativo busca atingir especificamente o sistema de informática alvo da ação criminosa.[44] Nas palavras de Marcelo Crespo:

> Crimes digitais próprios ou puros (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (hacking), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas; [...][45]

---

[42] COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

[43] TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico.** 6. ed. São Paulo: SaraivaJur, 2022. p. 224.

[44] LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** 2. ed. São Paulo: Atlas, 2011. p. 20.

[45] CRESPO, Marcelo Xavier de Freitas. Crimes Digitais: do que estamos falando? **Canal Ciências Criminais.** Disponível em: http://canalcienciascriminais.com.br/artigo/crimes-digitais-do-que-estamos-falando/. Acesso em: 28 jun. 2023.

Para Damásio de Jesus e Vladimir Aras:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.[46]

São condutas antijurídicas e culpáveis, com objetivo de causar dano a um sistema ou violar seus dados, afetando sua confiabilidade e integralidade.[47] Estes delitos demandam de uma atualização legislativa para criar novos tipos penais, uma vez que o alvo é o próprio sistema de informática e os computadores, ou sejam novos bens jurídicos que não são tutelados pela lei penal.[48]

Deste modo, uma vez observados os principais pontos sobre o uso da internet como meio para cometimento de crimes, o próximo capítulo irá abordar os crimes cibernéticos previstos no ordenamento jurídico brasileiro.

---

[46] JESUS, Damásio de. ARAS, Vladmir. Crimes de informática: Uma nova criminalidade. **JUS.** Disponível em: https://jus.com.br/artigos/2250/crimes-de-informatica. Acesso em: 23 out. 2023.

[47] SYDOW, Spencer Toth. **Delitos informáticos próprios:** uma abordagem sob a perspectiva vitimodogmática. Dissertação para o Departamento de Direito Penal, Medicina Forense e Criminologia. Universidade de São Paulo, 2009. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-15062011-161113/publico/Dissertacao_Mestrado_versao_final_formatada_padroes_US.pdf. Acesso em: 28 jun. 2023. p. 46.

[48] VIEIRA, Tatiana Malta. A convenção de Budapeste sobre crimes cibernéticos e o ordenamento jurídico nacional. **Revista de Direito de Informática e Telecomunicações.** v. 4, p. 197-232. Belo Horizonte, jan. 2009. p. 199.

3 OS CRIMES CIBERNÉTICOS PREVISTOS NO ORDENAMENTO JURÍDICO BRASILEIRO

Torna-se premente mencionar que o direito existe para regular as relações humanas, na qual a internet está presente, mesmo que de forma indireta. Ocorre que, o Código Penal é de 1940 e possui inúmeros bens jurídicos forjados em uma época em que não existiam os relacionamentos sociais como nos dias atuais.[49] Em que pese ser possível a utilização de algumas normas penais já existentes em crimes cometidos pela internet, é necessário reconhecer que existem crimes cibernéticos propriamente ditos, que demandam um tipo penal específico para serem punidos.[50]

3.1 ESTUPRO VIRTUAL

Nesta esteira, atualmente, um dos crimes já previstos no Código Penal, mas que passaram a ser cometidos por meio digital, foi o crime de estupro, sendo denominado de estupro virtual, que ocorre quando o agente, por meio de grave ameaça à vítima, exige que está faça determinada atividade que para a satisfação sexual do agente, mesmo que não ocorra o contato físico entre ambos.[51]

O primeiro caso de estupro virtual foi reproduzido pelo escritor Julian Dibell, que trouxe as formas como a violência e o abuso podem serem realizados através da internet, relatando que em 1933 ocorreu a primeira violência desse tipo, em que pese o primeiro caso ter sido julgado em 2017.[52] No Código Penal o crime de estupro está previsto no art. 213, que dispõe:

---

[49] MORAES, Alexandre Rocha Almeida de; SILVA, Isabella Tucci; SANTIAGO, Bruno. Os cibercrimes e a investigação digital: novos paradigmas para a persecução penal. **Momentum**, Atibaia, v. 1, n. 18, p. 1-34, 2020. Disponível em: https://momentum.emnuvens.com.br/momentum/article/download/284/201/557. Acesso em: 04 set. 2023.

[50] MORAES, Alexandre Rocha Almeida de; SILVA, Isabella Tucci; SANTIAGO, Bruno. Os cibercrimes e a investigação digital: novos paradigmas para a persecução penal. **Momentum**, Atibaia, v. 1, n. 18, p. 1-34, 2020. Disponível em: https://momentum.emnuvens.com.br/momentum/article/download/284/201/557. Acesso em: 04 set. 2023.

[51] COSTA, Fernando José da. Estupro Virtual. **ESTADÃO.** Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/estupro-virtual/. Acesso em: 27 ago. 2023.

[52] BARBOSA, Clara de Freitas. **Penal, processo penal, criminologia e novas tecnologias:** A caracterização jurídica do estupro virtual. Disponível em: http://conpedi.danilolr.info. Acesso em: 27 ago. 2023.

> Art. 213. Constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou a praticar ou permitir que com ele se pratique outro ato libidinoso:
> Pena - reclusão, de 6 (seis) a 10 (dez) anos.[53]

Nota-se que o próprio texto legal permite essa extensão quando praticado em meio virtual, ao dispor que o constrangimento pode ser aquele que ocorra por conjunção carnal ou por outro ato libidinoso. De acordo com Fernando Capez, a ameaça é considerada grave quando o dano prometido é maior que a própria conjunção carnal ou a prática do ato libidinoso, de forma que deve ser analisada sob o ponto de vista da vítima, tendo em vista as suas condições físicas e psíquicas.[54]

Nesse contexto, o agressor utiliza a internet, redes sociais, mensagens, e-mails ou outros meios online para coagir, ameaçar ou forçar a vítima a realizar atos sexuais ou para divulgar imagens íntimas contra a vontade dela.

3.2 PORNOGRAFIA DE VINGANÇA

Nessa mesma toada, tem-se que a prática da pornografia de vingança cresceu de forma exacerbada em relação aos crimes digitais, principalmente nos Estados Unidos em meados de 1980 por uma revista de conteúdo adulto, chamada Hustler, que continha um espaço para fotos amadoras enviadas por seus leitores, ocorre que, a imensa maioria dessas fotos eram das ex parceiras dos homens que enviavam, sem o consentimento das mesmas. [55]

Por essa razão, muitas demandas judiciais ocorreram contra a revista, mas uma vez que publicada as fotos, o dano às vítimas é irreparável, pois não há como controlar o compartilhamento das publicações. O termo “pornografia da vingança” ou “*revange porn”* consiste em divulgar em sites ou redes sociais fotos e vídeos de

---

[53] BRASIL. **Decreto-Lei n° 2.848, de 7 de dezembro de 1940.** Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 27 jul. 2023.
[54] CAPEZ, Fernando. **Curso de Direito Penal**. v. 3, parte especial: arts. 213 a 359-H, 17. ed. São Paulo: Saraiva Educação, 2019. p. 94.
[55] BURÉGIO, Fátima. Pornografia da vingança: Você sabe o que é isto. **JUSBRASIL.** Disponível em: https://ftimaburegio.jusbrasil.com.br/artigos/178802845/pornografiada-vinganca-voce-sabe-o-que-e-isto. Acesso em: 26 ago. 2023.

intimidade, nudez, sexo e similares, com a finalidade de colocar a pessoa em situação vexatória e constrangedora diante da sociedade com um propósito de vingança.[56]

Trata-se de uma causa de aumento de pena, de um a dois terços, se tratando da veiculação não consentida de mídia sexual que anteriormente foi feita de forma consentida, mas que divulgada após o término do relacionamento, cujo elemento subjetivo específico é a vingança ou a humilhação motivadora do crime.[57] A tipificação está no art. 218-C do Código Penal, com a causa de aumento de pensa prevista no §1°, que determinam:

> Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia:
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.
> Aumento de pena
> §1º A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação.[58]

Trata-se de uma prática que envolve o compartilhamento não consensual de imagens ou vídeos sexualmente explícitos de uma pessoa, muitas vezes após o término de um relacionamento, como uma forma de vingança, humilhação ou controle. Essa prática é profundamente prejudicial e invasiva, tendo graves implicações para a privacidade, a dignidade e a saúde emocional das vítimas, além de constituir uma violação a privacidade e aos direitos das vítimas.

3.3 ESTELIONATO VIRTUAL

Os primeiros crimes virtuais visavam sabotar os mecanismos informáticos, mas com a expansão da internet, surgiu a oportunidade para a prática de diferentes crimes.

---

[56] BURÉGIO, Fátima. Pornografia da vingança: Você sabe o que é isto. **JUSBRASIL.** Disponível em: https://ftimaburegio.jusbrasil.com.br/artigos/178802845/pornografiada-vinganca-voce-sabe-o-que-e-isto. Acesso em: 26 ago. 2023.

[57] JALIL, Mauricio Schaun; GRECO FILHO, Vicente; et al. **Código penal comentado:** doutrina e jurisprudência. 5. ed. Santana de Parnaíba: Manole, 2022. p. 708.

[58] BRASIL. **Decreto-Lei n° 2.848, de 7 de dezembro de 1940.** Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 27 jul. 2023.

Assim, os crimes virtuais tiveram uma rápida evolução, passando a englobar exposição de informações e imagens intimas, roubo e estelionato.

O crime de estelionato consiste na prática de golpes, em que os criminosos enganam as vítimas para obter algum tipo de vantagem, na maioria das vezes em dinheiro. Entretanto, com o avanço da tecnologia, os dispositivos eletrônicos possibilitaram novas formas de perpetrar o crime.[59] Em razão disso e visando coibir esse tipo de prática, a Lei n° 14.155/2021, que alterou o Código Penal, criando a figura da Fraude Eletrônica, nos § 2º-A, § 2º-B e § 3º do art. 171, que possibilitou um tratamento penal mais severo ao crime de estelionato, introduzindo uma qualificadora quando praticado por meio de fraude eletrônica, conforme explica-se:

> Sendo o estelionato um crime de forma vinculada (somente típico se praticado por meio de fraude), tem-se que a inserção da nova circunstância buscou punir de modo mais gravoso as condutas perpetradas com o recurso a meios de telecomunicação (diálogos telefônicos) e, também, a meios eletrônicos de comunicação e de interação social (redes sociais, mensagens eletrônicas etc.). Ademais, com o emprego da interpretação analógica, dada no caso pela expressão “outro meio fraudulento análogo”, resta autorizada ao hermeneuta a subsunção típica relativamente a condutas que, não expressamente mencionadas pela letra do dispositivo, com este guardem pertinência de sentido e finalidade, isto é, qualquer outro artifício ou ardil, executável no meio virtual ou de telecomunicação, idôneo a induzir a vítima ao erro, gerando a esta um prejuízo econômico e, em contrapartida, um lucro ilícito em favor do agente (p.ex., na hipótese de o estelionatário obter tais informações em plataformas virtuais controladas e mantidas para fins de ensino ou trabalho ou em fóruns restritos de jogos eletrônicos etc.). Constata-se, pois, que, malgrado a rubrica “fraude eletrônica”, possível o enquadramento típico para ações delitivas praticadas fora do ambiente virtual ou mesmo sem emprego de equipamento de informática, bastando que o agente se valha de um singelo aparelho telefônico ainda que desconectado da rede mundial de computadores.[60]

A diferença entre o estelionato comum e o praticado de forma eletrônica é encontrada no *modus operandi,* enquanto um ocorre no mundo físico, o outro se consuma com o uso de mecanismos informáticos. Assim, com a novidade legislativa, a redação do delito de estelionato ficou da seguinte forma:

---

[59]BRASIL. Estelionato. **Tribunal de Justiça do Distrito Federal e dos Territórios – TJDFT.** Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/estelionato-1#:~:text=O%20famoso%20crime%20do%20artigo,maioria%20da%20vezes%20em%20dinheiro. Acesso em: 28 jun. 2023.

[60] JALIL, Mauricio Schaun; GRECO FILHO, Vicente; *et al.* **Código penal comentado:** doutrina e jurisprudência. 5. ed. Santana de Parnaíba: Manole, 2022. p. 591.

> 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. (Vide Lei nº 7.209, de 1984)
> § 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.
> § 2º - Nas mesmas penas incorre quem:
> [...]
> Fraude eletrônica
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. (Incluído pela Lei nº 14.155, de 2021)
> § 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência
> § 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso..[61]

Victor Hugo Pereira Gonçalves descreve que para a configuração do estelionato eletrônico são necessários dois requisitos, quais sejam: que o agente empregue a fraude utilizando informações fornecidas pela vítima ou terceiro; e que tenha sido obtidas por meio de rede social, contato telefônico, correio eletrônico ou outro meio análogo.[62] Rogério Sanches Cunha exemplifica cada conduta descrita no artigo supramencionado, da seguinte forma:

> a) por meio de redes sociais: atualmente são muito comuns os anúncios promovidos em redes sociais como Facebook e Instagram. Não raro, são anúncios fraudulentos, manobras ardilosas para atrair pessoas que forneçam seus dados;
> b) por contatos telefônicos: são também muito comuns as fraudes cometidas por meio telefônico. Um exemplo recorrente envolve os cartões de crédito. O fraudador telefona para alguém e afirma, por exemplo, que a instituição financeira detectou indícios de fraude com o cartão dessa pessoa. Pede a ela que confirme dados e digite a senha do cartão. Com a senha à disposição, o agente faz compras, efetua saques, toma empréstimos etc.;
> c) pelo envio de correio eletrônico fraudulento: neste caso, a vítima recebe um e-mail fraudulento, muitas vezes imitando os caracteres de empresas ou organizações conhecidas e, a partir do acesso por meio do link disponibilizado, o estelionatário pode obter os dados pessoais e bancários inseridos em formulários eletrônicos;

---

[61] BRASIL. **Decreto-Lei n° 2.848, de 7 de dezembro de 1940.** Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 27 jul. 2023.
[62] GONÇALVES, Victor Hugo Pereira. **Direito penal – parte especial.** 13. ed. São Paulo: SaraivaJur, 2023. p. 234.

> d) por qualquer outro meio fraudulento análogo: nesta fórmula analógica se inserem quaisquer outras práticas fraudulentas cometidas por meios eletrônicos ou informáticos, como páginas na internet, por exemplo, em que a vítima não é diretamente abordada pelo estelionatário, como nas modalidades anteriores, mas é induzida em erro por fatores diversos (simulação de um estabelecimento comercial regularmente constituído; cópia de outra página conceituada etc.).[63]

Trata-se de uma outra modalidade de estelionato, concentrada no mercado de capitais, onde há as condutas de organizar, gerir, distribuir ou intermediar carteiras de investimentos ou operações de ativos digitais, que envolvem a obtenção de uma vantagem ilícita em detrimento do patrimônio da vítima.[64] A vítima, ao fornecer informações que possibilitam a prática do crime, integra o ardil preparado pelo agente que deseja obter vantagem ilícita.[65]

Nesse contexto, o estelionato eletrônico ocorre quando o agente engana a vítima por meio de redes sociais, contatos telefônicos, correio eletrônico falso ou qualquer outro meio fraudulento digital, capaz de fornecer dados confidenciais, como por exemplo, senhas de acesso ou números de cartão de crédito ou débito.[66] Mostrando assim, como é fácil nos dias atuais cometer esses crimes virtuais devido à dificuldade de se chegar até o infrator. Sobre o mesmo aspecto o autor Mirabete, leciona:

> [...] protege-se ainda uma vez com o dispositivo a inviolabilidade patrimonial e, também a boa-fé, segurança, fidelidade e veracidade dos negócios jurídicos patrimoniais, embora esta apareça em caráter secundário, já que o estelionato é um crime contra o patrimônio.[67]

---

[63] CUNHA, Rogério Sanches. Lei 14.155/21 e os crimes de fraude digital: primeiras impressões e reflexos no CP e no CPP. **Juspodivm,** 2021. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/. Acesso em: 28 jun. 2023.

[64] NUCCI, Guilherme de Souza. **Curso de direito penal:** parte especial – arts. 121 a 212 do Código Penal. 7. ed. Rio de Janeiro: Forense, 2023. p. 398.

[65] CUNHA, Rogério Sanches. Lei 14.155/21 e os crimes de fraude digital: primeiras impressões e reflexos no CP e no CPP. **Juspodivm,** 2021. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/. Acesso em: 28 jun. 2023.

[66] BRASIL. Estelionato. **Tribunal de Justiça do Distrito Federal e dos Territórios – TJDFT.** Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/estelionato-1#:~:text=O%20famoso%20crime%20do%20artigo,maioria%20da%20vezes%20em%20dinheiro. Acesso em: 28 jun. 2023.

[67] MIRABETE, Julio Fabbrini. **Manual de direito penal: parte especial:** arts. 121 a 234-B do CP / Julio Fabrinni Mirabete. Renato N. Fabrinni. – 35. Ed. – São Paulo: Atlas, 2019. p.295.

Atualmente, todos utilizam aplicativos para realizar transações e acessar documentos, guardando em aparelhos telefônicos dados pessoais e financeiros, que tornam caracterizam um cenário propício para a prática do estelionato digital. Desse modo, cabe ao Direito Penal ingressar nesse campo para ampliar a sua tutela e trazer meios de punição para estes criminosos, adaptando-se a necessidade contemporânea.[68]

3.4 FURTO QUALIFICADO POR MEIO INFORMÁTICO

Diferencia-se do estelionato virtual, o crime de furto qualificado por meio informático, previsto no art. 155, §4-B e §4-C do Código Penal, que ocorre quando o furto é cometido mediante fraude por meio de dispositivo eletrônico ou informático, com ou sem violação de mecanismo de segurança ou com a utilização de programa malicioso, cuja pena é de 4 a 8 anos de reclusão.[69] Tais dispositivos foram introduzidos no Código Penal através da Lei n° 14.155/2021, que ficaram com as seguintes redações:

> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
> Pena - reclusão, de um a quatro anos, e multa.
> [...]
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso
> I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.

Trata-se da subtração de bens móveis alheios por meio de fraude, utilizando dispositivos eletrônicos ou informáticos, a qual, de acordo com a definição legal, não

---

[68] NUCCI, Guilherme de Souza. **Curso de direito penal:** parte especial – arts. 121 a 212 do Código Penal. 7. ed. Rio de Janeiro: Forense, 2023. p. 399.

[69] CAMPELO, Marcelo. Crimes Cibernéticos - Furto Qualificado por Meio Informático - Art. 155 §4-B e §4-C - Código Penal. **JUS.** Disponível em: https://www.jusbrasil.com.br/artigos/crimes-ciberneticos-furto-qualificado-por-meio-informatico-art-155-4-b-e-4-c-codigo-penal/1778770536. Acesso em: 29 out. 2023.

importa se o referido dispositivo está ou não conectado à internet, nem se ocorre ou não uma violação de qualquer mecanismo de segurança existente. Entretanto, a falta de conexão com a internet reduz consideravelmente a gravidade desse ato criminoso, uma vez que a ausência de conexão virtual diminui o potencial dano que essa conduta poderia causar.[70]

Assim como no estelionato virtual, o furto qualificado por meio informático visa coibir a prática daqueles que se valem do uso tecnológico para cometer crimes, principalmente em detrimento da população que não possui conhecimento suficiente sobre o funcionamento de tais delitos.[71]

É importante fazer uma distinção entre o crime de furto mediante fraude através de dispositivo eletrônico ou informático e o crime de estelionato cibernético ou virtual. No primeiro, o objeto é subtraído, e a fraude é utilizada como um meio de enganar a vigilância ou a atenção da vítima, de forma que a fraude serve apenas como um meio para efetuar a subtração do bem. Por outro lado, no estelionato cibernético ou virtual, a vítima entrega voluntariamente seu bem como resultado da fraude cometida pelo agente. Nesse caso, a fraude precede a apropriação do bem e serve para enganar a vítima e levá-la a entregar o bem voluntariamente. Portanto, no estelionato virtual, a vítima desempenha um papel ativo, ou terceiros fornecem as informações necessárias para a prática da fraude, sendo induzidos ao erro por meio de redes sociais, contatos telefônicos, envio de correio eletrônico fraudulento ou por qualquer outro meio fraudulento similar.[72]

---

[70] BITENCOURT, Cezar Roberto. Furto mediante uso de dispositivo eletrônico ou informático. **CONJUR.** Disponível em: https://www.conjur.com.br/2021-jun-14/bitencourt-furto-mediante-uso-dispositivo-eletronico-ou-informatico. Acesso em: 30 out. 2023.

[71] CAMPELO, Marcelo. Crimes Cibernéticos - Furto Qualificado por Meio Informático - Art. 155 §4-B e §4-C - Código Penal. **JUS.** Disponível em: https://www.jusbrasil.com.br/artigos/crimes-ciberneticos-furto-qualificado-por-meio-informatico-art-155-4-b-e-4-c-codigo-penal/1778770536. Acesso em: 29 out. 2023.

[72] ANDREUCCI, Ricardo Antonio. Furto mediante fraude por meio de dispositivo eletrônico ou informático. **Empório do Direito.** Disponível em: https://emporiododireito.com.br/leitura/furto-mediante-fraude-por-meio-de-dispositivo-eletronico-ou-informatico. Acesso em: 30 out. 2023.

3.4 CALÚNIA, INJÚRIA E DIFAMAÇÃO

Estes três delitos tutelam a honra da pessoa, seja em seu aspecto objetivo, que diz respeito à reputação que a vítima possui em um contexto social, ou em seu aspecto subjetivo, que se refere ao sentimento da própria dignidade ou decoro.[73]

O crime de calúnia, previsto no art. 138 do Código Penal consiste em imputar falsamente a alguém fato definido como crime, ou seja, acusar alguém de ter praticado um fato criminoso. [74] Nesses termos, dispõe referido artigo:

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
> § 2º - É punível a calúnia contra os mortos.

Miguel Reale Júnior descreve: "[...] atribui-se inveridicamente a uma pessoa crime por ela não perpetrado, o que vulnera a honra objetiva do ofendido, ou seja, sua reputação ou sua imagem no corpo social. A falsidade pode referir-se tanto ao próprio fato como à sua autoria [...]".[75]

No que tange ao crime de difamação, este diferente da calúnia, ocorre quando é imputado um fato ofensivo à reputação, a qual não precisa necessariamente ser falsa, tampouco precisa caracterizar crime.[76] Assim, o Código Penal tipifica no art. 139: "Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa". Desse modo, tem-se que "Difamar significa "causar má fama", razão pela qual o objeto jurídico em questão é a honra objetiva, ou seja, a reputação ou a imagem da pessoa perante a sociedade [...]".[77]

No crime de injúria, por sua vez, a ofensa não é manifestada com a imputação de fato determinado, mas sim por meio de qualquer forma de expressão depreciativa a respeito da vítima, podendo ocorrer por meio de palavras, escritas, gestos,

---

[73] REALE JÚNIOR, Miguel. **Código penal comentado.** 2. ed. São Paulo: SaraivaJur, 2023. p. 225.
[74] JALIL, Mauricio Schaun; GRECO FILHO, Vicente; et al. **Código penal comentado:** doutrina e jurisprudência. 5. ed. Santana de Parnaíba: Manole, 2022. p. 424.
[75] REALE JÚNIOR, Miguel. **Código penal comentado.** 2. ed. São Paulo: SaraivaJur, 2023. p. 226.
[76] JALIL, Mauricio Schaun; GRECO FILHO, Vicente; et al. **Código penal comentado:** doutrina e jurisprudência. 5. ed. Santana de Parnaíba: Manole, 2022. p. 433.
[77] REALE JÚNIOR, Miguel. **Código penal comentado.** 2. ed. São Paulo: SaraivaJur, 2023. p. 227.

desenhos, imagens e outras formas.[78] Assim, considera-se que “Injúria é a ofensa à dignidade (isto é, moralidade) ou ao decoro de alguém (ou seja, aspectos físicos e intelectuais)”.[79]

O crime está previsto no art. 140 do Código Penal, que dispõe:

> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa.
> § 1º - O juiz pode deixar de aplicar a pena:
> I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;
> II - no caso de retorsão imediata, que consista em outra injúria.
> § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:
> Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.
> § 3º Se a injúria consiste na utilização de elementos referentes a religião ou à condição de pessoa idosa ou com deficiência:
> Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Estes crimes quando praticados de forma virtual, tem suas penas aumentadas em um terço em razão da ofensividade da ação,[80] com previsão do §2°, art. 141 do Código Penal, que determina:

> Art. 141 - As penas cominadas neste Capítulo aumentam-se de um terço, se qualquer dos crimes é cometido:
> [...]
> § 2º Se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena.[81]

Na internet, esses crimes podem ocorrer em diversas plataformas, como redes sociais, blogs, fóruns, mensagens instantâneas e e-mails, sendo de difícil responsabilização penal em razão da anonimidade e à natureza global da rede.

---

[78] JALIL, Mauricio Schaun; GRECO FILHO, Vicente; et al. **Código penal comentado:** doutrina e jurisprudência. 5. ed. Santana de Parnaíba: Manole, 2022. p. 436.

[79] REALE JÚNIOR, Miguel. **Código penal comentado.** 2. ed. São Paulo: SaraivaJur, 2023. p. 228.

[80] REALE JÚNIOR, Miguel. **Código penal comentado.** 2. ed. São Paulo: SaraivaJur, 2023. p. 231.

[81] BRASIL. **Decreto-Lei n° 2.848, de 7 de dezembro de 1940.** Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 27 jul. 2023.

3.5 INVASÃO DE DISPOSITIVOS

O crime de invasão de dispositivos foi introduzido no ordenamento jurídico brasileiro através das Leis n° 12.735/12 e 12.737/12, que alteraram o Código Penal e acrescentaram o seguinte artigo[82]:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 1° Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
> § 3° Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
> § 4° Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5° Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.[83]

Trata-se de crime comum, onde o sujeito ativo e passivo pode ser qualquer. Além disso, são crimes que não necessitam de um resultado material, onde a invasão do dispositivo é admitido na forma tentada e somente suportado na forma dolosa da conduta.[84] Este delito fere principalmente o que preceitua a Constituição Federal, em relação às garantias fundamentais previstas no *caput* do art. 5°, que determina:

---

[82] COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

[83] BRASIL. **Decreto-Lei n° 2.848, de 7 de dezembro de 1940.** Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 27 jul. 2023.

[84] COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

“Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...]”.[85]

Como visto, a criminalidade pelo meio eletrônico pode ocorrer de diversas formas, de modo que, a política criminal não pode ficar anacrônica, devendo atender às expectativas da dogmática penal contemporânea e promover meios de investigação condizentes com o atual cenário para proteger os bens penalmente tutelados e repreender novas condutas.[86]

Nesse cenário, são necessárias novas técnicas de investigação, pois os métodos tradicionais muitas vezes são insuficientes e ineficazes para o enfrentamento dos crimes cibernéticos.[87]

Outrossim, o próximo capítulo irá abordar os mecanismos de investigação de crimes cibernéticos, onde serão analisadas as principais legislações sobre o tema e as dificuldades enfrentadas pela polícia judiciária na investigação de crimes cometidos através da internet.

---

[85] BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 jul. 2023.

[86] MORAES, Alexandre Rocha Almeida de; SILVA, Isabella Tucci; SANTIAGO, Bruno. Os cibercrimes e a investigação digital: novos paradigmas para a persecução penal. **Momentum**, Atibaia, v. 1, n. 18, p. 1-34, 2020. Disponível em: https://momentum.emnuvens.com.br/momentum/article/download/284/201/557. Acesso em: 04 set. 2023.

[87] BUFFON, Jaqueline Ana. Agente infiltrado virtual. In: BRASIL. **Crimes cibernéticos.** 2ª Câmara de Coordenação e Revisão, Criminal. Ministério Público Federal. Brasília: MPF, 2018. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 25 out. 2023. p. 76.

4 MECANISMOS DE INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS

O direito é um meio que orienta a vida em sociedade através dos instrumentos legais, onde a legislação deve ser observada e aplicada, assim como ser atualizada de acordo com a atual sociedade, sendo necessário que os aplicadores do direito proporcionem aos agentes condições de buscar resultados satisfatórios e trabalhos especializados.[88]

Nesse contexto, o presente capítulo visa analisar os meios de investigação de crimes cibernéticos, onde serão abordados os meios investigatórios na legislação vigente, as previsões no Marco Civil da Internet, na Lei Carolina Dieckmann e no Código Penal e Processo Penal, bem como, serão analisadas as dificuldades de investigação e repressão dos crimes cibernéticos.

4.1 MEIOS INVESTIGATÓRIOS NA LEGISLAÇÃO VIGENTE

Atualmente, há uma grande necessidade em regulamentar o uso da internet, uma vez que os fatos cotidianos estão sendo colocados no mundo virtual, de modo que, é imprescindível que o Direito acompanhe a evolução da sociedade e traga meios para combater a lesão a bens jurídicos tutelados.[89] Nesse sentido, Roberto Antônio Darós Malaquias dispõe:

> Desta forma percebe-se que o impacto social das atividades criminosas no espaço cibernético está diretamente ligado ao crescente aumento do número de pessoas que passam a utilizar as novas tecnologias, inclusive empresas privadas e órgãos governamentais que usam a internet para obter inúmeras soluções, desde o campo da pesquisa acadêmica até o mais sofisticado comércio eletrônico. Os dados estatísticos demonstram o crescimento e a popularização do acesso à rede mundial de computadores.[90]

---

[88] COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

[89] COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

[90] MALAQUIAS, Roberto Antônio Darós. **Crime Cibernético e prova:** a investigação criminal em busca da verdade. 1. ed. Curitiba: Juruá, 2012, p. 53.

As transformações proporcionadas pela internet geraram certa perplexidade nas pessoas, que não sabiam ao certo como comportar-se nesse cenário digital, imaginando que a internet seria uma “terra sem lei”, onde tudo seria permitido, principalmente em razão da aparente anonimidade. Percebeu-se então, uma deficiência legislativa para combater certos problemas que surgiram junto com o uso da internet pela sociedade.[91]

4.1.1 Lei Carolina Dieckmann

A Lei n° 12.735/12 foi uma das primeiras a ser criada em razão da necessidade de especialidade para o combate de crimes cibernéticos, surgindo a polícia especializada, bem como, passou a tipificar as condutas realizadas mediante o uso de sistema eletrônico, digital ou similar, no art. 154-A do Código Penal[92], que ficou com a seguinte redação:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita [...][93]

Posteriormente foi publicada a Lei n° 12.737/12, conhecida como Lei Carolina Dieckmann, que passou a criminalizar a invasão de computadores, o roubo de senhas e arquivos, tipificando delitos cibernéticos ao acrescentar os Arts. 154-A e 154-B ao Código Penal, nos crimes previstos contra a liberdade individual, em razão de uma invasão no computador e a divulgação de imagens íntimas da atriz na internet, o que

---

[91] TOMASEVICIUS FILHO, Eduardo. Marco civil da internet: uma lei sem conteúdo normativo. **Estudos Avançados,** Atualidades. v. 30 (86). Jan-Apr 2016. Disponível em: https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/. Acesso em: 28 jun. 2023.

[92] COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

[93] BRASIL. **Decreto-Lei n° 2.848, de 7 de dezembro de 1940.** Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 27 jul. 2023.

causou grande repercussão na mídia e as fotos foram divulgadas pelas redes sociais.[94]

Desse modo, a Lei Carolina Dieckmann auxilia pessoas que tiveram sua privacidade invadida, criada para diferenciar a função da tecnologia auxilia pessoas que tem sua vida privada invadida, e foi criada para diferenciar as funções da tecnologia informática como um meio para o cometimento de crimes.

4.1.2 Marco Civil da Internet

Com o advento da Lei n° 12.965/14, conhecida como Marco Civil da Internet, foi possível uma posição mais clara acerca da proteção jurídica da liberdade de expressão e da privacidade no ambiente virtual, através de uma disposição principiológica que estabelecem parâmetros gerais de direitos, garantias e deveres para o uso da internet no Brasil.[95] Nas palavras de Victor Hugo Pereira Gonçalves:

> O Marco Civil é uma legislação cujo objetivo precípuo é o de regular as relações sociais entre os usuários de internet. A internet é um fenômeno tecnológico recente que alterou a forma das relações e a percepção social de situações que, no mundo físico, seriam simples e banais. Um simples comentário, depreciativo ou não, emitido na rua, propagava-se e perdia-se naquele momento. O mesmo comentário, na internet, fixa-se indefinidamente nos programas e servidores dela, que nunca se esquecerão e registrarão aquele simples evento para sempre. Esta transição que estamos vivenciando entre a fugacidade do mundo atual para a perenidade da memória, sempre real e vívida, do virtual, faz que as relações sociais, históricas, políticas e econômicas sejam vistas com novas percepções, desdobramentos e amplificações [...].[96]

O objetivo da Lei é promover o direito de acesso à internet e à informação, ao conhecimento e à participação na vida cultural e política, promover a inovação tecnológica e permitir a comunicação e acessibilidade. Para isso, assegura o reconhecimento da escala mundial da rede, os direitos humanos, o desenvolvimento

---

[94] COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

[95] TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico.** 6. ed. São Paulo: SaraivaJur, 2022. p. 41.

[96] GONÇALVES, Victor Hugo Pereira. **Marco civil da internet comentado.** 1. ed. São Paulo: Atlas, 2017. p. 7.

da personalidade e o exercício da cidadania em meios digitais, a pluralidade, a abertura, colaboração, livre iniciativa, livre concorrência e a defesa do consumidor, bem como, a finalidade social da rede.[97] Dentre os princípios que norteiam o regime jurídico do uso da internet pelo Marco Civil, estão a garantia da liberdade de expressão, comunicação e manifestação de pensamento; proteção da privacidade; proteção dos dados pessoais; preservação e garantia da neutralidade de rede; preservação de estabilidade, segurança e funcionalidade da rede; responsabilização dos agentes; preservação da natureza participativa da rede; e liberdade de negócios.[98]

4.1.3 Previsão no Código de Processo Penal

Com a elaboração do Projeto de Lei Anticrime n° 882/2019, propôs-se a alteração da Lei n° 12.850/13, introduzindo, pela primeira vez, o conceito de "cadeia de custódia" na legislação brasileira. No entanto, o diploma legal não reconhecia a importância da autenticidade e de formalidades específicas, o que contrariava a essência da cadeia de custódia. Assim, o sucesso da aprovação do Projeto consistiria principalmente na inclusão desse instituto no sistema legal do país, apesar de contrariar a sua própria definição.[99]

Contudo, não havia ainda legislação com dispositivos que regulamentavam a necessidade de registrar e preservar os elementos de prova usados nos processos, tampouco que estabelecessem as repercussões da não conformidade com essas disposições.[100] Por esse motivo, a regulamentação da cadeia de custódia foi incorporada à legislação por meio da Lei n° 13.964/2019, também conhecida como o "Pacote Anticrime", após um esforço de discussão interinstitucional e interdisciplinar,

---

[97] TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico.** 6. ed. São Paulo: SaraivaJur, 2022. p. 42.

[98] TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico.** 6. ed. São Paulo: SaraivaJur, 2022. p. 43.

[99] ÁVILA, Gustavo Noronha de; BORRI, Luiz Antonio. A cadeia de custódia da prova no “projeto de lei anticrime”: suas repercussões em um contexto de encarceramento em massa. **Direito Público**, v. 16, m. 89. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3592. Acesso em: 23 out. 2023.

[100] VIEIRA, Antonio. A cadeia de custódia da prova no processo penal: algumas notas sobre as alterações promovidas pela lei 13.964/2019 (pacote anticrime). **Boletim Revista do Instituto Baiano de Direito Processual Penal,** n. 7, fev. 2020.

o que refletiu na inclusão dos artigos 158-A a 158-F no Código de Processo Penal, os quais estabelecem um conjunto abrangente de diretrizes que definem esse instituto.[101]

A inclusão da cadeia de custódia da prova no Código de Processo Penal representou um significativo avanço na legislação brasileira, pois passou a estabelecer a integridade do instituto como um meio de garantir a autenticidade das evidências e assegurar que a prova examinada seja aquela associada ao incidente criminal em questão, o que reflete em um pressuposto epistemológico fundamental para o processo de produção de provas.[102]

Após a existência de um delito, uma das principais tarefas da polícia é a busca por vestígios, além de garantir o devido isolamento e preservação do local, o que é fundamental para evitar a perda dos vestígios e assegurar a autenticidade dos mesmos. Posteriormente, para que esses vestígios possam ser admitidos como provas em um processo, devem ser coletados de acordo com os princípios e procedimentos previamente estabelecidos, sendo crucial registrar todos os atos e pessoas que tiveram contato com as evidências, garantindo, assim, a integridade da prova por meio da cadeia de custódia. [103]

O primeiro artigo sobre a cadeia de custódia no Código de Processo Penal, art. 158-A, se preocupa em trazer uma definição ao instituto, considerando ser "[...] o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte".[104]

A definição estabelecida pelo legislador abrange, de fato, apenas a dimensão técnico-científica da cadeia de custódia, focando no processo que envolve a coleta, transporte, armazenamento, análise e interpretação do material a ser examinado. No

---

[101] GIACOMOLLI, Nereu José; AMARAL, Maria Eduarda Azambuja. A cadeia de custódia da prova pericial na lei n° 13.964/2019. **Revista Duc In Altum**, Cadernos de Direito, v. 12, n. 27, mai-ago 2020, p. 80.

[102] VIEIRA, Antonio. A cadeia de custódia da prova no processo penal: algumas notas sobre as alterações promovidas pela lei 13.964/2019 (pacote anticrime). **Boletim Revista do Instituto Baiano de Direito Processual Penal,** n. 7, fev. 2020.

[103] MACHADO, Michelle Moreira. Importância da cadeia de custódia da prova pericial. **RCML – Revista Criminalística e Medicina Legal,** v. 1, n. 2, 2017, p. 8-12, ISSN 2526-0596.

[104] BRASIL. **Decreto-lei n° 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 23 out. 2023.

entanto, esta definição deixa de considerar as etapas anteriores que caracterizam o aspecto processual, e, portanto, é vista como insuficiente e limitada.[105]

Os parágrafos do mencionado artigo estabelece que a cadeia de custódia tem início com a preservação do local do crime ou com procedimentos realizados por agentes policiais ou periciais sempre que sejam identificados vestígios. Nesse contexto, vestígios são definidos como qualquer objeto ou material, tanto visível quanto latente, que tenha relação com a infração penal. Além disso, é determinado que o agente público que identificar um elemento a ser utilizado como evidência pericial assume a responsabilidade pela sua preservação.[106]

A definição apresentada está relacionada à documentação da cadeia de custódia, uma vez que o termo "cadeia de custódia" se refere à sequência de indivíduos que tiveram contato com a fonte de prova real, desde o momento em que foi coletada até ser apresentada ao tribunal. Isso envolve o registro e a documentação de todas as etapas e pessoas envolvidas no manuseio e na preservação da evidência, garantindo sua integridade e autenticidade ao longo do processo.[107] A cadeia de custódia da prova é um sistema de controle epistemológico essencial para a reconstrução histórica dos eventos e para garantir o devido processo legal. Ela assegura que o objeto de prova percorra um caminho monitorado entre as instâncias de exame, órgãos, departamentos e inspeções antes de ser incluído no processo por meio de relatórios. Isso é fundamental para manter a integridade e autenticidade das provas ao longo de seu trajeto no sistema legal.[108]

A principal finalidade da cadeia de custódia é assegurar a autenticidade da prova, garantindo que o elemento coletado seja o mesmo que será utilizado na decisão judicial. Isso proporciona segurança técnica e legal, certificando a origem dos vestígios de acordo com os níveis de confiança dos exames periciais. Dessa forma, as partes envolvidas no processo têm a garantia de que o Estado cumprirá a obrigação

---

[105] GIACOMOLLI, Nereu José; AMARAL, Maria Eduarda Azambuja. A cadeia de custódia da prova pericial na lei n° 13.964/2019. **Revista Duc In Altum**, Cadernos de Direito, v. 12, n. 27, mai-ago 2020, p. 82.

[106] BRASIL. **Decreto-lei n° 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 23 out. 2023.

[107] BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, 2019, n. 343, p. 7-10. Disponível em: https://www.ibccrim.org.br/js/pdf-js/web/viewer.html?file=/media/publicacoes/arquivos_pdf/revista-31-05-2021-10-44-29-869137.pdf. Acesso em: 23 out. 2023.

[108] GIACOMOLLI, Nereu José; AMARAL, Maria Eduarda Azambuja. A cadeia de custódia da prova pericial na lei n° 13.964/2019. **Revista Duc In Altum**, Cadernos de Direito, v. 12, n. 27, mai-ago 2020, p. 72.

de preservar a prova, garantindo sua integridade e confiabilidade, e também garantindo que a prova apresentada em juízo seja a mesma que foi originalmente coletada. [109]

O art. 158-B, por sua vez, se ocupa em descrever e definir uma série de condutas a serem adotadas de acordo com as etapas do processo de documentação da cadeia de custódia, tratando em cada um dos incisos o que se deve entender por reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte de evidências.[110] Dessa forma, a cadeia de custódia da prova começa no momento da coleta do vestígio no local do crime e termina com o trânsito em julgado da decisão. Durante esse intervalo, é fundamental seguir os procedimentos legais relativos à coleta, acondicionamento, preservação e armazenamento a fim de assegurar a integridade, autenticidade e confiabilidade dos elementos de prova. [111]

Através da cadeia de custódia da prova, o processo de documentação pode assegurar a identidade, integridade e autenticidade dos elementos probatórios e contraprovas, reduzindo os riscos de erro judiciário. Isso garante que o mesmo elemento encontrado no local do crime seja aquele utilizado para embasar a decisão judicial, fortalecendo assim a confiabilidade e a justiça do sistema legal.[112]

As garantias proporcionadas pela cadeia de custódia permitem a preservação do local onde ocorreu a infração penal, conferindo maior confiabilidade à prova. Isso é essencial, uma vez que muitos vestígios têm a tendência de desaparecer facilmente, tornando impossível sua reprodução na fase processual. Portanto, esses vestígios podem ser tratados com rigor técnico e científico para manter sua integridade e confiabilidade. Além disso, todos os procedimentos realizados, juntamente com as

---

[109] GIACOMOLLI, Nereu José; AMARAL, Maria Eduarda Azambuja. A cadeia de custódia da prova pericial na lei n° 13.964/2019. **Revista Duc In Altum**, Cadernos de Direito, v. 12, n. 27, mai-ago 2020, p. 74.

[110] VIEIRA, Antonio. A cadeia de custódia da prova no processo penal: algumas notas sobre as alterações promovidas pela lei 13.964/2019 (pacote anticrime). **Boletim Revista do Instituto Baiano de Direito Processual Penal,** n. 7, fev. 2020.

[111] GIACOMOLLI, Nereu José; AMARAL, Maria Eduarda Azambuja. A cadeia de custódia da prova pericial na lei n° 13.964/2019. **Revista Duc In Altum**, Cadernos de Direito, v. 12, n. 27, mai-ago 2020, p. 76.

[112] ÁVILA, Gustavo Noronha de; BORRI, Luiz Antonio. A cadeia de custódia da prova no “projeto de lei anticrime”: suas repercussões em um contexto de encarceramento em massa. **Direito Público**, v. 16, m. 89. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3592. Acesso em: Acesso em: 23 out. 2023.

pessoas que tiveram contato com o material, podem ser devidamente documentados e registrados.[113]

A previsão do art. 158-E em relação à implementação de uma central de custódia nos Institutos de Criminalística foi acertada por parte do legislador. Isso ocorreu porque os laboratórios de perícia geralmente não dispõem de espaço físico adequado para essa finalidade. Portanto, é crucial ter uma central de controle dedicada a receber, armazenar, transferir e conduzir contra perícias, o que reforça a importância de garantir a integridade, autenticidade e confiabilidade das provas, contribuindo para um processo legal justo e seguro.[114]

De acordo com o artigo mencionado, a central de custódia deve estar equipada com um serviço de protocolo, um local para conferência, recepção e devolução de materiais e documentos. Além disso, deve registrar a entrada e saída de vestígios, documentando todas as informações relevantes no inquérito. Também é fundamental registrar todas as pessoas que tiveram acesso aos vestígios armazenados. Esses procedimentos permitem uma rastreabilidade completa da cadeia de custódia, demonstrando a transparência de todo o processo de produção de provas. Isso, por sua vez, garante a integridade das provas em todas as fases da investigação e do processo penal.[115]

A cadeia de custódia exige o estabelecimento de um procedimento regrado e formalizado, no qual seja possível documentar de forma cronológica existencial da fonte de prova, permitindo assim a posterior validação em juízo e o exercício do controle epistêmico, o que implica na adoção de metodologias adequadas que garantam a preservação do instituto.[116]

De acordo com os dispositivos legais mencionados, fica evidente que a cadeia de custódia tem início com a preservação do local do crime, evitando qualquer

---

[113] CARVALHO, Jefferson Lemes. Cadeia de custódia e sua relevância na persecução penal. **Brazilian Journal of Forensic Sciencies, Medical Law and Bioethics**, v. 5, n. 4, p. 371-382, 2016. Disponível em: http://dx.doi.org/10.17063/bjfs5(4)y2016371. Acesso em: 23 out. 2023.

[114] GIACOMOLLI, Nereu José; AMARAL, Maria Eduarda Azambuja. A cadeia de custódia da prova pericial na lei n° 13.964/2019. **Revista Duc In Altum**, Cadernos de Direito, v. 12, n. 27, mai-ago 2020, p. 90.

[115] CARVALHO, Jefferson Lemes. Cadeia de custódia e sua relevância na persecução penal. **Brazilian Journal of Forensic Sciencies, Medical Law and Bioethics**, v. 5, n. 4, p. 371-382, 2016. Disponível em: http://dx.doi.org/10.17063/bjfs5(4)y2016371. Acesso em: 23 out. 2023.

[116] RUTTKE, Alberto Milnickel; AMARAL, Maria Eduarda Azambuja. Breves reflexões sobre a cadeia de custódia da prova: a metodologia utilizada no exame pericial como critério essencial à admissibilidade da prova pericial. In: **Direito e liberdade:** estudos em homenagem ao professor doutor Nereu José Giacomolli. São Paulo: Almedina, 2022, p. 568.

contaminação ou destruição de vestígios cruciais. O propósito é assegurar que os elementos de prova apresentados ao juiz sejam os mesmos que foram encontrados na cena do crime, de forma a garantir que não tenham sido adulterados. Isso é alcançado por meio dos procedimentos estipulados na legislação. Com essa abordagem, é possível garantir que a prova submetida ao tribunal seja, de fato, a mesma que foi tratada como vestígio no local do crime, assegurando a integridade da prova material.[117]

Todos esses procedimentos são essenciais para prevenir a manipulação indevida de provas com o intuito de incriminar ou absolver alguém de responsabilidade, visando alcançar a melhor qualidade na tomada de decisão judicial e impedindo injustiças. Além disso, buscam estabelecer de maneira objetiva um processo que garanta a integridade das provas, independentemente das questões relacionadas ao elemento subjetivo do agente. Isso presume a legitimidade de todos os atos e exige que qualquer conduta criminosa e os motivos que levariam uma autoridade a manipular uma prova sejam devidamente demonstrados.[118]

4.2 PERÍCIA COMPUTACIONAL

Atualmente, os dispositivos utilizados pela sociedade são objetos tecnológicos, desde eletrodoméstico até os smartphones, os quais possuem capacidade de processamento e controle embutido, possibilitando usabilidade, eficiência e segurança aos usuários. O núcleo desses equipamentos são os microcontroladores com unidades de processamentos adaptáveis.[119]

Os pesquisadores de segurança digital possuem grande potencial para fazer mudanças importantes para as forenses digitais, permitindo uma melhor eficácia nas investigações. No entanto, é preciso entender as limitações que podem afetar os contextos investigatórios.[120]

---

[117] EDINER, Carlos. Cadeia de custódia, rastreabilidade probatória. **Revista Brasileira de Ciências Criminais**, v. 24, n. 120, p. 237–257, maio/jun., 2016.

[118] LOPES JÚNIOR, Aury. **Direito processual penal.** 19. ed. São Paulo: SaraivaJur, 2022, p. 191.

[119] SAVOINE, Marcia Maria; SILVA, Fernanda Rosa da. **Investigação remota de sistemas e técnicas de evasão.** São Paulo: Platos Soluções Educacionais S.A, 2021. p. 6.

[120] CAIADO, Felipe B.; CAIADO, Marcelo. Combate à pornografia infanto-juvenil com aperfeiçoamento na identificação de suspeitos e na detecção de arquivos de interesse. *In:* BRASIL. **Crimes cibernéticos.** 2ª Câmara de Coordenação e Revisão, Criminal. Ministério Público Federal. Brasília:

Nos casos de crimes cibernéticos, a perícia é a melhor fonte para identificar a materialidade e autoria do delito, a qual geralmente é realizada em fase policial, em razão da urgência. Marcia Maria Savoine e Fernanda Rosa da Silva destacam que toda evidencia digital válida é orientada por três pilares, quais sejam:

> • Relevância: a evidência é tida como relevante quando se propõe a provar ou negar itens de um caso específico em investigação.
> • Confiabilidade: consiste em garantir que a evidência digital seja o que foi designada a ser. Isso significa que ela deve estar íntegra e verossímil em seu conteúdo.
> • Suficiência: conceito que compreende que a evidência digital tenha quantidade necessária, ou seja, suficiente, para torná-la convincente.[121]

A obtenção de provas digitais são cruciais para a elucidação dos delitos, principalmente quando existem diferentes jurisdições nas quais as evidências estão armazenadas.[122]Ao coletar dados de dispositivos utilizados para o cometimento de crimes, é importante executar a recolha dele, averiguar o local do crime e leva-lo para um laboratório para aquisição e análise. Essa sequência de atos culminará na cadeia de custódia e na adequação da proteção do dispositivo.[123]

O processo de coleta de dados se inicia com a cópia da evidência digital a partir da extração dos dados ali presentes, que estão gravados na memória do dispositivo, para um arquivo ou outra máquina, cuidando para manter a integridade dos dados para que não haja questionamento sobre o objeto apreendido.[124]

> Na etapa de preservação da potencial evidência digital em dispositivos embarcados, é imprescindível saber manipular e acondicionar os artefatos de maneira que seja reduzida a probabilidade da espoliação ou adulteração, devido à natureza frágil desses dispositivos. Neste sentido, a espoliação pode acontecer a partir de uma degradação magnética ou elétrica, podendo ocorrer por motivos de temperatura elevada, exposição à alta ou baixa umidade e por choques e vibrações.

MPF, 2018. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 25 out. 2023. p. 11.

[121] SAVOINE, Marcia Maria; SILVA, Fernanda Rosa da. **Investigação remota de sistemas e técnicas de evasão.** São Paulo: Platos Soluções Educacionais S.A, 2021. p. 13.

[122] DOMINGOS, Fernanda Teixeira Souza; RODER, Priscila Costa Schreiner. Obtenção de provas digitais e jurisdição na internet.. In: BRASIL. **Crimes cibernéticos.** 2ª Câmara de Coordenação e Revisão, Criminal. Ministério Público Federal. Brasília: MPF, 2018. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 25 out. 2023. p. 27.

[123] SAVOINE, Marcia Maria; SILVA, Fernanda Rosa da. **Investigação remota de sistemas e técnicas de evasão.** São Paulo: Platos Soluções Educacionais S.A, 2021. p. 15.

[124] SAVOINE, Marcia Maria; SILVA, Fernanda Rosa da. **Investigação remota de sistemas e técnicas de evasão.** São Paulo: Platos Soluções Educacionais S.A, 2021. p. 16.

> Já a adulteração pode acontecer devido a uma ação proposital de alterar ou consentir na modificação da evidência digital. Então, é importante manipular as evidências digitais originais o mínimo possível e trabalhar sempre com as cópias realizadas, visando à preservação da integridade do dispositivo embarcado.[125]

O trabalho pericial especializada demanda profundos conhecimentos técnicos e de constantes atualizações para que o profissional execute o labor, respondendo juridicamente pelo resultado apresentado.[126] Sob a ótica jurídica, essa questão de perícia computacional, imprescindível destacar os arts. 156 a 158 do Código de Processo Civil que dispõem:

> Art. 156. O juiz será assistido por perito quando a prova do fato depender de conhecimento técnico ou científico.
> § 1º Os peritos serão nomeados entre os profissionais legalmente habilitados e os órgãos técnicos ou científicos devidamente inscritos em cadastro mantido pelo tribunal ao qual o juiz está vinculado. […]
> Art. 157. O perito tem o dever de cumprir o ofício no prazo que lhe designar o juiz, empregando toda sua diligência, podendo escusar-se do encargo alegando motivo legítimo. […]
> Art. 158. O perito que, por dolo ou culpa, prestar informações inverídicas responderá pelos prejuízos que causar à parte e ficará inabilitado para atuar em outras perícias no prazo de 2 (dois) a 5 (cinco) anos, independentemente das demais sanções previstas em lei, devendo o juiz comunicar o fato ao respectivo órgão de classe para adoção das medidas que entender cabíveis.[127]

Durante todo esse processo é importante que as ações sejam documentadas através da cadeia de custódia, que identificará a ordem cronológica de todo movimento e manipulação da evidência, [128] conforme amplamente dissertado anteriormente.

---

[125] SAVOINE, Marcia Maria; SILVA, Fernanda Rosa da. **Investigação remota de sistemas e técnicas de evasão.** São Paulo: Platos Soluções Educacionais S.A, 2021. p. 16.

[126] CAIADO, Felipe B.; CAIADO, Marcelo. Combate à pornografia infanto-juvenil com aperfeiçoamento na identificação de suspeitos e na detecção de arquivos de interesse. *In:* BRASIL. **Crimes cibernéticos.** 2ª Câmara de Coordenação e Revisão, Criminal. Ministério Público Federal. Brasília: MPF, 2018. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 25 out. 2023. p. 15.

[127] BRASIL. **Decreto-lei n° 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 23 out. 2023.

[128] SAVOINE, Marcia Maria; SILVA, Fernanda Rosa da. **Investigação remota de sistemas e técnicas de evasão.** São Paulo: Platos Soluções Educacionais S.A, 2021. p. 16.

4.3 DIFICULDADES DE INVESTIGAÇÃO E REPRESSÃO DOS CRIMES CIBERNÉTICOS

O combate aos crimes cibernéticos apresenta desafios únicos para as autoridades, uma vez que muitas vezes envolvem fronteiras internacionais, além da capacidade dos criminosos de permanecerem anônimos e usarem tecnologias avançadas para mascarar sua identidade. A Polícia Judiciária é uma instituição de direito público destinada a manter a paz pública e a segurança da sociedade, com atuação preventiva e repressiva para disciplinar, regular e fiscalizar direitos e interesses sociais[129], cujas atribuições estão previstas no art. 144 da Constituição Federal, que dispõe:

> Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos:
> I - polícia federal;
> II - polícia rodoviária federal;
> III - polícia ferroviária federal;
> IV - polícias civis;
> V - polícias militares e corpos de bombeiros militares.
> VI - polícias penais federal, estaduais e distrital.
> [...]
> § 4º Às polícias civis, dirigidas por delegados de polícia de carreira, incumbem, ressalvada a competência da União, as funções de polícia judiciária e a apuração de infrações penais, exceto as militares.
> [...]
> § 7º A lei disciplinará a organização e o funcionamento dos órgãos responsáveis pela segurança pública, de maneira a garantir a eficiência de suas atividades. [...][130]

As investigações policiais através das diligências realizadas no Inquérito Policial são de suma importância para a efetividade na apuração dos delitos, especialmente os cibernéticos, que possuem especificidades e recursos adequados.[131]

---

[129] COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

[130] BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 jul. 2023.

[131] COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

A Lei de Organização de Investigação Criminal, Lei n° 49/2008, em seu art. 1°, define a investigação criminal como sendo: “[...] o conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as provas, no âmbito do processo”.[132]

A polícia vem conseguindo reprimir o cometimento de alguns crimes cibernéticos através do IP dos computadores, tendo em vista que este facilita a descoberta da localização do infrator e, consequentemente, sua identidade acaba podendo ser revelada. No entanto, as instituições apresentam dificuldades quanto à modernização da gestão e de aparatos qualificados e especializados que atendam as demandas desses delitos, que em razão de sua natureza, necessitam de tecnologias mais sofisticadas.[133]

> É salutar que a principal questão quanto à investigação policial, como já abordado, seria em relação ao desenvolvimento tecnológico, que demanda dos profissionais especialização na área, além da consideração de que há um excesso de tutela penal. Inclusive, a própria Lei nº 12.735/2012 previu no seu artigo 4º que “os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado”.[134]

As tecnologias de informação e comunicação apresentam uma complexidade e dinamismo extremos, o que, por outro lado, resulta na falta de preparo e qualificação adequados dos órgãos legislativos, de investigação e judiciários para enfrentar essa nova forma de criminalidade.[135] Portanto, a questão que se destaca em relação aos crimes cibernéticos está em grande parte relacionada à escassez de pessoal, à falta

---

[132] BRASIL. **Lei n° 49/2008.** Aprova a Lei de Organização da Investigação Criminal. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1021&tabela=leis&so_miolo=. Acesso em: 04 set. 2023.

[133] COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

[134] COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

[135] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. **JUS.** Disponível em: https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indiciosda-autoria-e-prova-da-materialidade. Acesso em: 24 out. 2023.

de atenção dada à capacitação e especialização dos agentes públicos e à carência de tecnologia adequada.[136]

O combate a esse tipo de criminalidade exige profissionais especializados, com instrumentos específicos para atuar com provedores de acesso e de conteúdo, instituições bancárias e representantes de redes sociais.[137] Se faz necessário que o aparelhamento estatal tenha mais investimentos e desenvolvimentos na área investigativa, seja em especialização dos agentes ou em equipamentos informáticos, para uma melhor prestação jurisdicional à sociedade.[138]

O relatório da CPI de Crimes Cibernéticos, publicado em 2016, apontou a necessidade urgente de investimentos na área de perícia com a apresentação de projetos de lei que visam uma melhor tipificação para alguns crimes, além de auxiliar na fase investigatória pelos entes públicos.[139]

---

[136] CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. **Revista científica eletrônica do curso de direito.** 13. ed. Disponível em: http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso em: 24 out. 2023.

[137] MORAES, Alexandre Rocha Almeida de; SILVA, Isabella Tucci; SANTIAGO, Bruno. Os cibercrimes e a investigação digital: novos paradigmas para a persecução penal. **Momentum**, Atibaia, v. 1, n. 18, p. 1-34, 2020. Disponível em: https://momentum.emnuvens.com.br/momentum/article/download/284/201/557. Acesso em: 04 set. 2023.

[138] COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

[139] CAIADO, Felipe B.; CAIADO, Marcelo. Combate à pornografia infanto-juvenil com aperfeiçoamento na identificação de suspeitos e na detecção de arquivos de interesse. *In:* BRASIL. **Crimes cibernéticos.** 2ª Câmara de Coordenação e Revisão, Criminal. Ministério Público Federal. Brasília: MPF, 2018. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 25 out. 2023. p. 14.

CONSIDERAÇÕES FINAIS

Com a globalização e o avanço tecnológico, a internet se estabeleceu como o principal meio de comunicação e acesso à informação para a população global. No entanto, apesar das facilidades proporcionadas pelo ambiente tecnológico, o mundo virtual também se tornou um local de risco devido à proliferação de novos delitos e à adaptação dos crimes preexistentes para o meio digital.

A evolução tecnológica e a acessibilidade à internet permitiram que criminosos se aproveitassem do anonimato e da disponibilidade de informações pessoais online para perpetrar crimes virtuais. Nesse contexto, a falta de uma tipificação adequada para todos os delitos cometidos no ambiente virtual e a velocidade das inovações tecnológicas dificultam a efetiva proteção contra os crimes cibernéticos.

Nesse contexto, o capítulo 2 abordou o uso da internet como meio para o cometimento de crimes, onde foi possível contextualizar a utilização da Internet e os desafios jurídicos, em razão do rápido avanço tecnológico, a utilização desenfreada da internet muitas vezes entra em conflito com direitos fundamentais, como a dignidade, intimidade, honra e imagem, além do direito à liberdade de expressão, de modo que a globalização da internet criou um ambiente em que alguns crimes passaram a ser cometidos virtualmente.

Dessa forma, se faz necessário uma maior regulamentação jurídica para manter a paz social, promover o desenvolvimento das relações e preservar o Estado Democrático de Direito, sendo essencial que o sistema legal se adapte às novas demandas decorrentes desse novo cenário virtual. Isso porque, as inovações tecnológicas frequentemente exigem alterações nas leis para lidar com novas situações e objetivos jurídicos, sendo importante conciliar essas mudanças com a manutenção da liberdade individual e dos princípios do Estado de Direito.

A internet, apesar de trazer inúmeros benefícios, também deu origem a uma série de crimes cometidos em ambientes virtuais, de forma que o Código Penal e outras legislações penais foram afetados por essa nova realidade, o que levou o legislador brasileiro a tipificar novas condutas e adaptar crimes já existentes. Os crimes cibernéticos frequentemente ocorrem com um senso de anonimato por parte dos autores, enquanto as vítimas podem se sentir seguras devido à falta de percepção clara dos riscos, isso cria desafios na investigação e na persecução penal, já que identificar os autores pode ser difícil.

O capítulo aborda também o surgimento dos primeiros crimes cibernéticos, como os vírus eletrônicos, trojans e worms, os quais têm evoluído ao longo do tempo, com o surgimento de novas tecnologias e ferramentas que facilitam a prática criminosa, sendo classificados em duas categorias: crimes cibernéticos impróprios, nos quais a informática é apenas uma ferramenta, e crimes cibernéticos próprios, nos quais o sistema de informática é o alvo principal.

No capítulo 3 foram destacados os principais crimes cibernéticos previstos no ordenamento jurídico brasileiro, abordando a necessidade de regulamentar os delitos relacionados à internet e às novas formas de relacionamento social no contexto atual, destacando que o Código Penal, não contempla as complexidades dos crimes cibernéticos.

Foi explorado o conceito de estupro virtual, que se refere a casos em que um agente, por meio de grave ameaça, força a vítima a realizar atividades de natureza sexual, mesmo sem contato físico direto. O crime de estupro no Código Penal (art. 213) é mencionado como uma base legal que pode ser aplicada a casos de estupro virtual. Também foi discutido o crime conhecido como pornografia de vingança, que envolve divulgar fotos ou vídeos íntimos de uma pessoa sem o seu consentimento, muitas vezes com o objetivo de humilhá-la ou se vingar, com previsão no art. 218-C do Código Penal, que tipifica esse crime, prevendo um aumento de pena se houver relação de afeto com a vítima ou se o ato for motivado por vingança.

Em seguida, foi visto sobre o crime de estelionato virtual, que envolve enganar vítimas para obter vantagens, através do ambiente digital, que surgiu com a Lei n° 14.155/2021, a qual introduziu a figura do "Estelionato Eletrônico" no Código Penal, com penas mais severas quando o crime for cometido por meio de fraude eletrônica, incluindo a obtenção de informações da vítima por meio de redes sociais, contatos telefônicos ou correio eletrônico fraudulento.

Foram abordados os crimes contra a honra: calúnia (acusar alguém falsamente de cometer um crime), difamação (imputar fatos ofensivos à reputação) e injúria (ofender a dignidade da pessoa), destacando como esses crimes podem ser agravados em um terço quando cometidos nas redes sociais ou na internet, de acordo com o §2° do art. 141 do Código Penal.

E por fim, o crime de invasão de dispositivos, inserido pelo art. 154-A no Código Penal, que envolve a violação de dispositivos informáticos alheios para obter, alterar

ou destruir dados sem autorização, com penas que aumentam se houver prejuízo econômico.

O capítulo 4 se ocupou em discutir os mecanismos de investigação de crimes cibernéticos e abordar várias questões relacionadas à legislação, à perícia computacional e às dificuldades enfrentadas na investigação e repressão desses crimes.

Foi visto a necessidade de regulamentar o uso da internet devido à crescente importância da tecnologia em nossas vidas, destacando a Lei Carolina Dieckmann, Lei n° 12.737/12, que tipificou crimes cibernéticos e invasões de computadores, fornecendo uma base legal para lidar com essas questões. Bem como, o Marco Civil da Internet, Lei n° 12.965/14, abordando o seu papel na proteção da liberdade de expressão e privacidade online.

Discutiu-se a inclusão do conceito de cadeia de custódia na legislação brasileira por meio da Lei n° 13.964/2019, conhecida como "Pacote Anti Crime ", a qual é considerada um processo fundamental para garantir a autenticidade e a integridade das evidências em investigações criminais.

Em relação a perícia computacional, foi visto sua importância na elucidação de crimes cibernéticos e a forma como os peritos forenses podem garantir que as evidências digitais sejam relevantes, confiáveis e suficientes, enfatizando a necessidade de preservar a integridade das evidências digitais ao coletá-las e manipulá-las.

Por fim, destacou-se as dificuldades enfrentadas pelas autoridades policiais na investigação de crimes cibernéticos, principalmente pela falta de recursos, conhecimento técnico especializado e equipamentos adequados, sendo necessário maiores investimentos por parte do Estado, em busca de modernização da gestão e de recursos para combater esse tipo de criminalidade, bem como a importância de uma regulamentação legal eficaz.

Dessa forma, o presente Trabalho de Conclusão de Curso demonstrou a necessidade de atualização constante da legislação e do desenvolvimento de competências e recursos especializados para combater eficazmente os crimes cibernéticos e garantir a integridade do processo judicial. Nesse contexto, confirma-se a hipótese básica apresentada na introdução do trabalho, de que o ordenamento jurídico brasileiro não possui mecanismos de investigação suficientes para investigar e combater os crimes cibernéticos.

REFERÊNCIAS

ANDRADE, Mariah Dourado de; BENTES, Dorinethe dos Santos; GUIMARAES, David Franklin da Silva. Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais. **Revista Vertentes do Direito.** Disponível em: https://redib.org/Record/oai_articulo1568032-considera%C3%A7%C3%B5es-sobre-a-aplicabilidade-do-direito-penal-acerca-dos-crimes-virtuais. Acesso em: 28 jun. 2023.

ÁVILA, Gustavo Noronha de; BORRI, Luiz Antonio. A cadeia de custódia da prova no “projeto de lei anticrime”: suas repercussões em um contexto de encarceramento em massa. **Direito Público**, v. 16, m. 89. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3592. Acesso em: 23 out. 2023.

BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, 2019, n. 343, p. 7-10. Disponível em: https://www.ibccrim.org.br/js/pdf-js/web/viewer.html?file=/media/publicacoes/arquivos_pdf/revista-31-05-2021-10-44-29-869137.pdf. Acesso em: 23 out. 2023.

BARBOSA, Clara de Freitas. **Penal, processo penal, criminologia e novas tecnologias:** A caracterização jurídica do estupro virtual. Disponível em: http://conpedi.danilolr.info. Acesso em: 27 ago. 2023.

BITENCOURT, Cezar Roberto. Furto mediante uso de dispositivo eletrônico ou informático. **CONJUR.** Disponível em: https://www.conjur.com.br/2021-jun-14/bitencourt-furto-mediante-uso-dispositivo-eletronico-ou-informatico. Acesso em: 30 out. 2023.

BRASIL. **Crimes cibernéticos. Brasília:** Ministério Público Federal, 2018. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 28 jun. 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 jul. 2023.

BRASIL. **Decreto-Lei n° 2.848, de 7 de dezembro de 1940.** Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 27 jul. 2023.

BRASIL. **Decreto-lei n° 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 23 out. 2023.

BRASIL. Estelionato. **Tribunal de Justiça do Distrito Federal e dos Territórios – TJDFT.** Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/estelionato-

1#:~:text=O%20famoso%20crime%20do%20artigo,maioria%20da%20vezes%20em%20dinheiro. Acesso em: 28 jun. 2023.

BRASIL. **Lei n° 49/2008.** Aprova a Lei de Organização da Investigação Criminal. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1021&tabela=leis&so_miolo=. Acesso em: 04 set. 2023.

BRASIL. **Crimes cibernéticos.** 2ª Câmara de Coordenação e Revisão, Criminal. Ministério Público Federal. Brasília: MPF, 2018. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 25 out. 2023.

BRASIL. **Projeto de Lei n° 882/2019.** Câmara dos Deputados. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2192353. Acesso em: 23 out. 2023.

BURÉGIO, Fátima. Pornografia da vingança: Você sabe o que é isto. **JUSBRASIL.** Disponível em: https://ftimaburegio.jusbrasil.com.br/artigos/178802845/pornografiada-vinganca-voce-sabe-o-que-e-isto. Acesso em: 26 ago. 2023.

CAMPELO, Marcelo. Crimes Cibernéticos - Furto Qualificado por Meio Informático - Art. 155 §4-B e §4-C - Código Penal. **JUS.** Disponível em: https://www.jusbrasil.com.br/artigos/crimes-ciberneticos-furto-qualificado-por-meio-informatico-art-155-4-b-e-4-c-codigo-penal/1778770536. Acesso em: 29 out. 2023.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. **Âmbito Jurídico.** Disponível em http://www.ambitojuridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17. Acesso em: 28 jun. 2023.

CARVALHO, Jefferson Lemes. Cadeia de custódia e sua relevância na persecução penal. **Brazilian Journal of Forensic Sciencies, Medical Law and Bioethics**, v. 5, n. 4, p. 371-382, 2016. Disponível em: http://dx.doi.org/10.17063/bjfs5(4)y2016371. Acesso em: 23 out. 2023.

CAPEZ, Fernando. **Curso de Direito Penal.** v. 3, parte especial: arts. 213 a 359-H, 17. ed. São Paulo: Saraiva Educação, 2019.

CASTRO, Carla Rodrigues Araújo. **Crimes de informática e seus aspectos processuais.** 2. ed. Rio de Janeiro: Lumen Juris, 2001.

COSTA, Emanuely Silva; SILVA, Raíla da Cunha. Crimes cibernéticos e investigação penal. **Revista Eletrônica do Ministério Público do Estado do Piauí**, ano 01, ed. 02, jul/dez 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 ago. 2021.

COSTA, Fernando José da. Estupro Virtual. **ESTADÃO.** Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/estupro-virtual/. Acesso em: 27 ago. 2023.

CRESPO, Marcelo Xavier de Freitas. Crimes Digitais: do que estamos falando? **Canal Ciências Criminais.** Disponível em: http://canalcienciascriminais.com.br/artigo/crimes-digitais-do-que-estamos-falando/. Acesso em: 28 jun. 2023.

CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. **Revista científica eletrônica do curso de direito.** 13. ed. Disponível em: http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf . Acesso em: 24 out. 2023.

CUNHA, Rogério Sanches. Lei 14.155/21 e os crimes de fraude digital: primeiras impressões e reflexos no CP e no CPP. **Juspodivm,** 2021. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/. Acesso em: 28 jun. 2023.

DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. **JUS.** Disponível em: https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indiciosda-autoria-e-prova-da-materialidade. Acesso em: 24 out. 2023.

D'URSO, Filizzola Luiz. Em Tempos de Cibercrimes. **Migalhas**, 2019. Disponível em: https://www.migalhas.com.br/dePeso/16,MI310551,31047-Em+tempos+de+cibercrimes. Acesso em: 28 jun. 2023.

EDINER, Carlos. Cadeia de custódia, rastreabilidade probatória. **Revista Brasileira de Ciências Criminais**, v. 24, n. 120, p. 237–257, maio/jun., 2016.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital e a sociedade da informação.** 2. ed. São Paulo: Saraiva, 2016.

FREITAS, Victor Valério Medeiros Siqueira de; SANTOS, Waldiney Batista dos; CURY, Leticia Vivianne Miranda Cury. Crimes virtuais: um olhar sob a ótica do direito penal. **Revista Ibero- Americana de Humanidades, Ciências e Educação-REASE**, v.9.n.05. mai. 2023. ISSN - 2675 – 3375. Disponível em: https://periodicorease.pro.br/rease/article/download/9868/3846/14568. Acesso em: 23 jul. 2023.

FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. Crimes Na Internet: elementos para uma reflexão sobre a ética informacional - **R. CEJ,** Brasília, n. 20, p. 67-73, jan./mar. 2003 Disponível em: https://revistacej.cjf.jus.br/cej/index.php/revcej/article/view/523. Acesso em: 23 out. 2023.

GIACOMOLLI, Nereu José; AMARAL, Maria Eduarda Azambuja. A cadeia de custódia da prova pericial na lei n° 13.964/2019. **Revista Duc In Altum**, Cadernos de Direito, v. 12, n. 27, mai-ago 2020.

GONÇALVES, Victor Hugo Pereira. **Direito penal – parte especial.** 13. ed. São Paulo: SaraivaJur, 2023.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital:** transformação digital: desafios para o direito. 2. ed. Rio de Janeiro: Forense, 2022.

JALIL, Mauricio Schaun; GRECO FILHO, Vicente; et al. **Código penal comentado:** doutrina e jurisprudência. 5. ed. Santana de Parnaíba: Manole, 2022.

JESUS, Damásio de; OLIVEIRA, José Antonio Milagre de. **Manual de crimes informáticos.** 1. ed. São Paulo: Saraiva, 2016.

JESUS, Damásio de. ARAS, Vladmir. Crimes de informática: Uma nova criminalidade. **JUS.** Disponível em: https://jus.com.br/artigos/2250/crimes-de-informatica. Acesso em: 23 out. 2023.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** 2. ed. São Paulo: Atlas, 2011.

LOPES JÚNIOR, Aury. **Direito processual penal.** 19. ed. São Paulo: SaraivaJur, 2022.

MACHADO, Michelle Moreira. Importância da cadeia de custódia da prova pericial. **RCML – Revista Criminalística e Medicina Legal**, v. 1, n. 2, 2017, p. 8-12, ISSN 2526-0596.

MALAQUIAS, Roberto Antônio Darós. **Crime Cibernético e prova:** a investigação criminal em busca da verdade. 1. ed. Curitiba: Juruá, 2012.

MARTINI, Kelly de; LACERDA, Emanuela Cristina Andrade. O direito, a informática e a sociedade**. Revista do Curso de Direito da FSG,** ano 6, n. 11, jan./jun. 2012, p. 53-61. Disponível em: https://ojs.fsg.edu.br/index.php/direito/article/view/346/320. Acesso em: 28 jun. 2023.

MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Borges. Os Crimes Cibernéticos no Ordenamento Jurídico Brasileiro e a Necessidade de Legislação Específica. **GCP ADVOGADOS.** Disponível em: http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-ea-necessidade-de-legislacao-especifica-2. Acesso em: 23 out. 2023.

MIRABETE, Julio Fabbrini. **Manual de direito penal:** parte especial: arts. 121 a 234-B do CP. 35. ed. São Paulo: Atlas, 2019.

MONTEIRO, Neto. **Aspectos constitucionais e legais do crime eletrônico.** Dissertação de Pós-Graduação em Direito. Universidade de Fortaleza, 2008.

Disponível em: https://bdtd.ibict.br/vufind/Record/UFOR_35c4cc8a1b88754a2fbdd093192cf6dc. Acesso em: 28 jun. 2023.

MORAES, Alexandre Rocha Almeida de; SILVA, Isabella Tucci; SANTIAGO, Bruno. Os cibercrimes e a investigação digital: novos paradigmas para a persecução penal. **Momentum**, Atibaia, v. 1, n. 18, p. 1-34, 2020. Disponível em: https://momentum.emnuvens.com.br/momentum/article/download/284/201/557. Acesso em: 04 set. 2023.

NASCIMENTO, Samir de Paula. Cibercrime: conceitos, modalidades e aspectos jurídicos-penais. **Âmbito Jurídico.** Disponível em: https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitosmodalidades-e-aspectos-juridicos-penais/. Acesso em: 28 jun. 2023.

NUCCI, Guilherme de Souza. **Curso de direito penal:** parte especial – arts. 121 a 212 do Código Penal. 7. ed. Rio de Janeiro: Forense, 2023.

OLIVEIRA JUNIOR, Eudes Quintino. A nova lei Carolina Dieckmann. **Jusbrasil,** dez. 2012. Disponível em: https://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann. Acesso em: 28 jun. 2023.

PINHEIRO, Patrícia Peck. **Direito digital.** 7. ed. São Paulo: Saraiva, 2021.

REALE JÚNIOR, Miguel. **Código penal comentado.** 2. ed. São Paulo: SaraivaJur, 2023.

ROQUE, Sérgio Marcos. **Criminalidade Informática:** crimes e criminosos do computador. 1. ed. São Paulo: ADPESP Cultural, 2007.

RUTTKE, Alberto Milnickel; AMARAL, Maria Eduarda Azambuja. Breves reflexões sobre a cadeia de custódia da prova: a metodologia utilizada no exame pericial como critério essencial à admissibilidade da prova pericial. In: **Direito e liberdade:** estudos em homenagem ao professor doutor Nereu José Giacomolli. São Paulo: Almedina, 2022, p. 568.

SÁNCHEZ, Jésus-Maria Silva. **A expansão do direito penal: aspectos da política criminal na sociedade pós-industrial.** Traduzido por Luiz Otávio de Oliveira Rocha. São Paulo: Editora Revista dos Tribunais, 2002.

SAVOINE, Marcia Maria; SILVA, Fernanda Rosa da. **Investigação remota de sistemas e técnicas de evasão.** São Paulo: Platos Soluções Educacionais S.A, 2021.

SOUZA, Henry Leones de; VOLPE, Luiz Fernando Cassilhas. Da ausência de legislação específica para os crimes virtuais. **Revista Eletrônica da Faculdade de Direito de Alta Floresta**, v. 8, n. 2, 2015. Disponível em: https://egov.ufsc.br/portal/conteudo/da-aus%C3%AAncia-de-legisla%C3%A7%C3%A3o-espec%C3%ADfica-para-os-crimes-virtuais. Acesso em: 28 jun. 2023.

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática.** Dissertação para o Departamento de Direito Penal, Medicina Forense e Criminologia. Universidade de São Paulo, 2009. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-15062011-161113/publico/Dissertacao_Mestrado_versao_final_formatada_padroes_US.pdf. Acesso em: 28 jun. 2023.

TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico.** 6. ed. São Paulo: SaraivaJur, 2022.

TOMASEVICIUS FILHO, Eduardo. Marco civil da internet: uma lei sem conteúdo normativo. **Estudos Avançados, Atualidades.** v. 30 (86). Jan-Apr 2016. Disponível em: https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/. Acesso em: 28 jun. 2023.

VIEIRA, Tatiana Malta. A convenção de Budapeste sobre crimes cibernéticos e o ordenamento jurídico nacional. **Revista de Direito de Informática e Telecomunicações.** v. 4, p. 197-232. Belo Horizonte, jan. 2009.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos:** ameaças e procedimentos de investigação. 1. ed. São Paulo: Editora Brasport, 2012.