UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
DEPARTAMENTO DE DIREITO
CURSO DE DIREITO

MARIA EDUARDA PEREIRA VIEIRA

A ADESÃO DO BRASIL A CONVENÇÃO DE BUDAPESTE E A CORREÇÃO DAS DEFICIÊNCIAS LEGISLATIVAS QUANTO AOS CRIMES CIBERNÉTICOS

Florianópolis
2023

MARIA EDUARDA PEREIRA VIEIRA

A ADESÃO DO BRASIL A CONVENÇÃO DE BUDAPESTE E A CORREÇÃO DAS DEFICIÊNCIAS LEGISLATIVAS QUANTO AOS CRIMES CIBERNÉTICOS

Trabalho de Conclusão de Curso submetido ao curso de Direito do Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de Bacharela em Direito.

Orientadora: Prof.ª Liz Beatriz Sass, Dr.ª

Florianópolis

2023

MARIA EDUARDA PEREIRA VIEIRA

A Adesão do Brasil a Convenção de Budapeste e a Correção das deficiências Legislativas quanto aos Crimes Cibernéticos.

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do título de Bacharela e aprovado em sua forma final pelo Curso de Direito.
Florianópolis, 27 de junho de 2023.

Prof. Francisco Quintanilha Veras Neto, Dr.
Coordenação do Curso

Banca examinadora

Prof.ª Liz Beatriz Sass, Dr.ª
Orientadora

Ariê Scherreier Ferneda
Programa de Pós-Graduação em Direito (PPGD/UFSC)

Michelle de Medeiros Fidélis
Programa de Pós-Graduação em Direito (PPGD/UFSC)

Florianópolis, 2023

RESUMO

O objetivo deste trabalho de conclusão de curso é explorar a discussão sobre as múltiplas formas de criminalidade que emergem incessantemente no cenário digital, impulsionadas pela expansão constante da internet na sociedade contemporânea, bem como pela insuficiência da legislação pátria. Diante disso, este estudo tem como problemática discutir quais os impactos da adesão do Brasil à Convenção de Budapeste no que se refere ao combate ao crime cibernético, e assim contribuir para a compreensão de um fenômeno crescente e complexo que é a cibercriminalidade, e mais especificamente, as repercussões e desafios que surgem com a adesão, avaliando as transformações jurídicas e práticas decorrentes deste compromisso. No atual contexto de proliferação de delitos cibernéticos, foi realizada uma análise detalhada sobre as novas formas de criminalidade que emergem continuamente no ambiente digital. Assim, por meio do método de abordagem dedutivo, e de pesquisa bibliográfica e documental, a pesquisa foi estruturada em três capítulos. O primeiro analisa o surgimento do crime digital e seus tipos. O segundo capítulo trata do histórico da legislação nacional e a evolução dos cibercrimes ao mesmo tempo. E, por fim, o terceiro capítulo analisa as normas internas sobre cibercrime, a dificuldade de investigação frente à problemática do anonimato, e a legislação nacional, particularmente antes e após a adesão formal à Convenção de Budapeste, e discute os possíveis desafios advindos dessa adesão. Infere-se, pois que a hipótese foi corroborada, indicando que a legislação brasileira necessita de revisões, atualizações e ampliações, com foco especial nas peculiaridades do ambiente digital e nos delitos que ocorrem nesse espaço, ressaltando a necessidade de um equilíbrio cuidadoso entre a garantia da segurança cibernética e a preservação dos direitos individuais.

Palavras-chave: Crimes cibernéticos; Segurança cibernética; Cooperação internacional; Convenção de Budapeste; Insuficiência legislativa.

ABSTRACT

The objective of this course completion work is to explore the discussion about the multiple forms of criminality that continuously emerge in the digital scenario, driven by the constant expansion of the internet in contemporary society, as well as the insufficiency of domestic legislation. In light of this, this study aims to discuss the impacts of Brazil's adherence to the Budapest Convention in relation to combating cybercrime, and thus contribute to the understanding of a growing and complex phenomenon that is cybercriminality, and more specifically, the repercussions and challenges that arise with this adherence, evaluating the legal and practical transformations resulting from this commitment. In the current context of proliferation of cybercrimes, a detailed analysis was conducted on the new forms of criminality that continuously emerge in the digital environment. Thus, through the deductive approach method, and through bibliographic and documentary research, the study was structured into three chapters. The first chapter analyzes the emergence of digital crime and its types. The second chapter addresses the history of national legislation and the evolution of cybercrimes at the same time. And finally, the third chapter analyzes the internal norms on cybercrime, the investigative difficulties related to the issue of anonymity, and the national legislation, particularly before and after the formal adherence to the Budapest Convention, discussing the possible challenges arising from this adherence. It can be inferred, therefore, that the hypothesis was corroborated, indicating that Brazilian legislation needs revisions, updates, and expansions, with a special focus on the peculiarities of the digital environment and the crimes that occur in this space, highlighting the need for a careful balance between guaranteeing cybersecurity and preserving individual rights.

Keywords: Cybercrimes. Cybersecurity; International cooperation; Budapest Convention; Legislative insufficiency.

SUMÁRIO

1. INTRODUÇÃO

A globalização tecnológica aumentou exponencialmente o seu espaço na vida cotidiana das pessoas, consolidando-se como o principal sistema de comunicabilidade global, de forma quantitativa e qualitativa, com a possibilidade de comunicação instantânea e acesso a informações em todo o planeta, devido aos vastos recursos que facilitam a vida de seus adeptos. Entretanto, esse avanço também catalisou um novo palco para a prática de ilícitos, e a partir dessa disseminação, surge uma nova tipologia de delitos cibernéticos, explicitando o paradoxo deste espaço simultaneamente livre e desestabilizador. Logo, a universalidade do acesso à internet, que transcende as fronteiras geográficas e políticas, torna o controle pelos órgãos reguladores um desafio, fazendo dela um território vasto e insurgente à legislação, caracterizado pelo anonimato e pela ilegalidade, bem como apresenta-se como um meio democrático de interação social, acessível a muitos. Todavia, é imprescindível compreender que essa democratização não deve prejudicar a segurança jurídica ou a proteção dos direitos fundamentais. Portanto, a busca por soluções jurídicas deve ser capaz de dialogar com a complexidade da era digital, respeitando suas especificidades, sem abdicar dos princípios que regem a convivência em sociedade.

Dessa forma, mesmo que a internet apresente desafios diários, o Direito está em constante ajuste a essas mudanças, tendo em vista a natureza da evolução tecnológica, a sua velocidade e a facilidade com que as informações são compartilhadas, somadas ao anonimato proporcionado pela internet. Por isso, se mostra indispensável que as estratégias jurídicas sejam pensadas a longo prazo, sendo suficientemente abrangentes para resistir à passagem do tempo, mas flexíveis o suficiente para acomodar várias situações relacionadas ao mesmo tema.

Neste cenário, muitos cibercriminosos permanecem impunes, tornando a internet um faroeste digital onde a vontade dos criminosos prevalece sobre os direitos e opiniões alheias, frente a facilidade de acesso a internet livremente, com a intenção de causar danos pessoais ou patrimoniais.

Em resposta a este contexto, o Brasil vem se esforçando para adequar sua legislação ao ambiente virtual. A Lei Carolina Dieckmann, de 2012, é um dos exemplos disso, ao tipificar alguns dos crimes virtuais e se tornar um marco importante na proteção da privacidade e segurança digital. O país também aderiu à

Convenção de Budapeste, que estabelece medidas para prevenir e combater o cibercrime internacionalmente. No entanto, apesar dessas iniciativas, a legislação brasileira ainda enfrenta desafios para efetivar a justiça digital, como o rastreamento de crimes virtuais e a necessidade de aprimorar os mecanismos de segurança digital.

Diante desta problemática, o presente trabalho visa verificar a importância e os impactos da adesão do Brasil a Convenção de Budapeste, avaliando as transformações jurídicas e práticas decorrentes deste compromisso. Assim, por meio do método de abordagem dedutivo, e de pesquisas bibliográficas e documentais, a pesquisa foi estruturada em três capítulos.

Com isso, o primeiro capítulo analisa o surgimento do crime digital e seus tipos derivantes.

Por conseguinte, o segundo capítulo analisa o histórico da legislação nacional em relação à cibercriminalidade, verificando a evolução das respostas jurídicas, diante a insuficiência do ordenamento jurídico interno para lidar com os desafios e complexidades inerentes à criminalidade digital.

Por fim, o terceiro e último capítulo traz a problemática abordada no presente trabalho de forma mais específica. Neste ponto, analisa-se as normas internas, e os desafios da legislação cibernética brasileira, particularmente antes e após a adesão formal à Convenção de Budapeste em 2023, e discute os possíveis complicações advindos dessa adesão.

Logo, a proposta desta monografia é verificar quais os impactos da adesão do Brasil à Convenção de Budapeste no que se refere ao combate ao crime cibernético, e assim contribuir para a compreensão de um fenômeno crescente e complexo que é a cibercriminalidade, e mais especificamente, as repercussões e desafios que surgem com a adesão.

2. A EVOLUÇÃO DO CIBERCRIME: ANÁLISE DOS DELITOS CIBERNÉTICOS PRÓPRIOS E IMPRÓPRIOS.

A ascensão da tecnologia digital no século XXI trouxe consigo não apenas novas oportunidades, mas também novas formas de crimes, como o cibercrime. Assim, este capítulo pretende explorar a gênese e a progressão desse fenômeno contemporâneo que desafia a ordem legal global. Diante a análise de seu surgimento, e o rastreamento de seus primórdios até sua forma atual, a fim de entender melhor como ele se desenvolveu e se adaptou com o avanço da tecnologia. A discussão não se limitará a um mero relato histórico, mas também examinará como as categorias de crimes cibernéticos foram estruturadas, com um foco particular nos crimes cibernéticos próprios e impróprios.

2.1. ORIGENS DO CIBERCRIME

O advento da tecnologia digital e das redes de comunicação marcou o início do cibercrime. Esta evolução tecnológica intensificou a transformação da forma como comunicamos, produzimos e compartilhamos informações. No entanto, o ambiente digital também proporcionou um cenário favorável para atividades ilícitas, uma vez que as técnicas para explorar vulnerabilidades e cometer atos ilícitos evoluíram paralelamente. A acessibilidade da internet, combinada com nossa crescente dependência dela para atividades cotidianas, se tornou um atrativo para criminosos.

Nesse contexto, com a difusão da internet, surgiram criminosos altamente especializados na linguagem informática, dando origem a uma variedade de termos para se referir às infrações penais realizadas por meio de dispositivos conectados à rede mundial de computadores. Essas terminologias abrangem cibercrimes, crimes cibernéticos, crimes informáticos, crimes na internet, crimes virtuais, crimes digitais, entre outros[1]. Todos são sinônimos de ações criminosas que envolvem o uso de computadores e redes de computadores, incluindo ataques de negação de serviço

---

[1]JUNIOR, Júlio Cesar Alexandre. Cibercrime: um estudo acerca do conceito de crimes informáticos. **Revista Eletrônica da Faculdade de Direito de Franca.** Disponível em . Acesso em https://www.revista.direitofranca.br/index.php/refdf/article/view/602#:~:text=Cibercrime%20est%C3%A1%20associado%20ao%20%E2%80%9Cfen%C3%B3meno,12). Acesso. 10 abr. 2023

(DDoS), fraudes bancárias e espionagem cibernética. No entanto, vale ressaltar que nem todas as ações ilegais realizadas na internet são consideradas cibercrimes. Este é um termo amplo que engloba não só atividades criminosas em rede, mas também comportamentos ilegais como cyberbullying, difamação e assédio online.

A história do cibercrime teve início no final dos anos 70 e começo dos anos 80, com o surgimento dos primeiros computadores pessoais. Neste período, hackers começaram a explorar as possibilidades da rede e a desenvolver técnicas de invasão de sistemas e redes.

Na década de 90, o cibercrime se tornou uma ameaça mais significativa para a sociedade com a popularização da internet, evoluindo e se diversificando com a popularização da internet. Nessa década, Tim Berners-Lee, cientista, físico e professor britânico, desenvolveu o primeiro navegador e servidor web, o *World Wide Web* (mais tarde renomeado para *Nexus*)[2]. Em 6 de agosto de 1991, ele disponibilizou publicamente o primeiro website, que explicava o que era a *World Wide Web*, como funcionava e como outros poderiam criar páginas web e hospedá-las em servidores. A invenção de Tim Berners-Lee permitiu que a internet evoluísse rapidamente, tornando a troca de informações e a comunicação global muito mais fáceis e rápidas.

O crescente e lucrativo mercado da internet impulsionou o desenvolvimento de novas ferramentas e serviços, tornando a rede cada vez mais complexa e dinâmica. Hoje, a *World Wide Web* é parte integrante da vida moderna, usada por bilhões de pessoas em todo o mundo para variados propósitos, como comunicação, educação, comércio e entretenimento. Contudo, ela também serve como ferramenta para criminosos cibernéticos que utilizam uma ampla gama de técnicas para perpetrar crimes online, como *phishing, ransomware, malware*, entre outros. A natureza difícil de rastrear e punir da internet e das redes de computadores torna o ambiente virtual ainda mais atrativo para a prática de crimes cibernéticos.

No Brasil, a história da internet iniciou-se na década de 1980, desenvolvendo-se paralelamente à evolução global da internet e aos seus impactos na sociedade. Em 1988, a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e o Laboratório Nacional de Computação Científica (LNCC) estabeleceram a primeira conexão de rede no país, destinada a fins acadêmicos e

---

[2]DIANA, Daniela. **História da internet.** Disponível em https://www.todamateria.com.br/historia-dainternet/. Acesso em 14 abr. 2023

de pesquisa.[3] No mesmo ano, ocorreu o primeiro grande incidente de cibercrime, com o "*worm*", criado pelo estudante americano Robert Tappan Morris. O programa de Morris, tinha como objetivo inicial avaliar a extensão da internet, que se propagou mais rápido e amplamente do que o previsto, interrompendo os serviços em cerca de 6.000 computadores, o que correspondia a 10% dos servidores de internet da época.[4] Esse caso foi considerado o primeiro grande incidente de cibercrime e resultou na condenação de Morris sob a Lei de Fraude e Abuso de Computador dos Estados Unidos.

Em 1991, a Rede Nacional de Ensino e Pesquisa (RNP) foi criada pelo Ministério da Ciência e Tecnologia com o objetivo de conectar instituições de ensino e pesquisa em todo o Brasil. Em 1994, a RNP estabeleceu a primeira conexão permanente à internet no Brasil, integrando universidades, centros de pesquisa e outras instituições científicas e tecnológicas. Naquele mesmo ano, a Embratel criou a primeira conexão comercial ao *backbone* da internet, permitindo o acesso à rede por empresas e provedores de serviços. Assim, em 1995, a internet comercial iniciou suas operações no Brasil, com o aval do governo federal para que empresas privadas oferecessem serviços de conexão.[5] Nesse período, o acesso à internet era majoritariamente restrito à comunidade acadêmica e a certas empresas. Contudo, a *web* brasileira começou a ganhar popularidade com a criação de *websites,* portais de notícias, lojas online e serviços de e-mail. Com isso, houve o crescimento acelerado da internet brasileira no início dos anos 2000, impulsionado pela expansão das conexões de banda larga e pelo aumento da oferta de serviços e conteúdos online.

Na contemporaneidade, a rede mundial de conexão ultrapassa seus propósitos iniciais de comunicação e entretenimento, tornando-se uma plataforma poderosa e crucial para a economia global. Assim, ela se encontra entrelaçada em

---

[3] VALVERDE, Danielle Novaes de Siqueira. Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso**. Revista da ESMAPE.** Recife. v. 15. n. 32. p. 236.

[4] WINDER, Davey. **This 20-Year-Old Virus Infected 50 Million Windows Computers In 10 Days:** Why The ILOVEYOU Pandemic Matters In: 2020. FORBES, 2020. Disponível em: https://www.forbes.com/sites/daveywinder/2020/05/04/this-20-year-old-virus-infected-50-million-windows-computers-in-10-days-why-the-iloveyou-pandemic-matters-in2020/?sh=10aa7f8b3c7c. Acesso em: 15 mai. 2023

[5]VALVERDE, Danielle Novaes de Siqueira. Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso. **Revista da ESMAPE.** Recife. v. 15. n. 32. p. 236. jul./dez. 2010.

todas as esferas da vida, desde relações interpessoais até transações empresariais, passando por áreas governamentais, segurança pública, educação, saúde e cultura.

Diante disso, evidencia-se as palavras de Mendes e Vieira[6]:

> A sociedade da informação em rede traz consigo novos desafios para a sociedade e para o direito, em especial para o direito penal. Os crimes cometidos pela internet são praticados em ambiente internacional, com ofensores e vítimas em diferentes países. A falta de fronteiras e de limites geográficos para a prática de delitos cibernéticos acarreta problemas para as autoridades, que muitas vezes encontram dificuldades em determinar o local da prática criminosa, a jurisdição aplicável e a efetivação de medidas de investigação e repressão. [...] 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.[7]

Sob esse viés, a tecnologia da informação e comunicação se tornou um elemento essencial e insubstituível para o desenvolvimento social, mas traz consigo riscos significativos, como a possibilidade de ameaças e ataques cibernéticos, gerando insegurança e prejuízos.

Nesse contexto, uma das principais referências no Brasil, a advogada Patricia Peck, especialista em Direito Digital, aborda o cibercrime como um fenômeno crescente e preocupante no mundo contemporâneo[8]. A visão de Peck sobre o cibercrime envolve uma abordagem multifacetada, que inclui a atualização das leis, cooperação internacional, educação e conscientização da população, segurança da informação nas empresas e responsabilização dos provedores de serviços de internet.[9]

Frente a essa temática, verifica-se que o Código Penal Brasileiro já prevê algumas modalidades de cibercrime, como a invasão de dispositivos informáticos e a falsificação de documentos eletrônicos, mas ainda há muitas lacunas a serem

---

[6] MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Borges. **Os Crimes Cibernéticos no Ordenamento Jurídico Brasileiro e a Necessidade de Legislação Específica.** Disponível em http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e a-necessidade-de-legislacao-especifica-2. Acesso em 14 de abr.2023

[7] MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Borges. **Os Crimes Cibernéticos no Ordenamento Jurídico Brasileiro e a Necessidade de Legislação Específica.** Disponível em http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e a-necessidade-de-legislacao-especifica-2. Acesso em 14 de abr. 2023 .

[8] PINHEIRO, Patrícia Peck, Direito digital. 6.ed., atual. e ampl. São Paulo: Saraiva, 2016.

[9]SENADO. **Combate ao cibercrime é urgente, afirmam especialistas na CCT.** Disponível https://www12.senado.leg.br/noticias/materias/2021/12/15/combate-ao-cibercrime-e-urgente-afirmam-especialistas-na-cct.Acesso em 14 abr. 2023.

preenchidas, especialmente se considerar a rápida evolução tecnológica, posto que há um impacto significativo na economia, já que muitas empresas dependem da internet para conduzir seus negócios.

De acordo com um estudo da Confederação Nacional da Indústria (CNI), o prejuízo causado pelos crimes cibernéticos no Brasil chegou a R$ 45 bilhões em 2019. Esses crimes também afetam a privacidade e a segurança dos usuários, comprometendo informações pessoais e financeiras e potencialmente causando danos emocionais e psicológicos[10].

Sob essa perspectiva, se evidencia que um dos principais desafios para combater o cibercrime no Brasil, envolve a falta de conscientização pública sobre os riscos da internet, a escassez de recursos e a falta de especialistas em segurança cibernética. Segundo o levantamento de dados da Fortinet[11], o Brasil registrou no primeiro semestre de 2022, 31,5 bilhões de tentativas de ataques cibernéticos a empresas, um aumento de 94% em relação ao mesmo período no ano anterior, quando ocasionou 16,2 bilhões de registros, e uma das justificativas para que haja tantos ataques no país se vivifica no baixo investimento em cibersegurança no Brasil. Além disso, o Brasil é visto como um dos principais pontos de origem de ataques cibernéticos em todo o mundo, segundo um relatório da Kaspersky, empresa de segurança cibernética, o Brasil se coloca como responsável de 10% dos ataques cibernéticos globais.[12]

Neste contexto preocupante, Patrícia Peck enfatiza a necessidade de uma abordagem integrada para enfrentar esses desafios, envolvendo autoridades, empresas, instituições de pesquisa e a sociedade civil. A educação e a conscientização do público são fundamentais para prevenir crimes cibernéticos, bem como a cooperação internacional também é essencial, já que muitos criminosos operam em diferentes países, dificultando a investigação e punição.

---

[10]SENADO. **Comissão de Relações Exteriores e Defesa Nacional.** Disponível https://www25.senado.leg.br/web/atividade/notas-taquigraficas/-/notas/r/10148 Acesso. 18. mai.2023

[11] OLIVEIRA, Ingrid. **Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%.** Disponível em https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94

[12]KASPERSKY. **Brasil e os ataques de phishing por WhatsApp**. Disponível em https://www.kaspersky.com.br/blog/brasil-ataques-phishing-2022/20943. Acesso em 17 abr. 2023

Frente a isso, o Brasil já criou leis específicas para tratar de cibercrimes, como a Lei Carolina Dieckmann (Lei nº 12.737/2012)[13], e é signatário da Convenção de Budapeste, um tratado internacional que estabelece medidas contra o cibercrime. Essas medidas jurídicas serão exploradas com mais detalhes nos capítulos subsequentes deste estudo.

O surgimento do cibercrime representa um desafio único para a sociedade moderna. Como um fenômeno que transcende fronteiras nacionais, requer uma abordagem global para ser efetivamente combatido. Embora o Brasil esteja tomando medidas significativas para o seu combate, ainda há um longo caminho a percorrer. Logo, este capítulo buscará explorar como as categorias de crimes cibernéticos foram estruturadas, com foco nos crimes cibernéticos próprios e impróprios.

2.2. TIPOS DE CRIMES CIBERNÉTICOS

A ascensão da internet forneceu um novo palco para o desenrolar de atividades criminosas. A fácil utilização, a volatilidade dos dados, a acessibilidade global e o anonimato dos usuários convergem para fazer da rede um ambiente propício para a prática de delitos. Isso desafia as fronteiras geográficas, dificultando o controle e repressão por parte das autoridades. Com o constante surgimento de novas formas de delitos e condutas, uma definição exata de crimes cibernéticos ainda é um desafio.

Nesse cenário, a internet pode ser tanto o veículo como o alvo de infrações penais, como demonstra Emerson Wendt e Higor Vinicius Nogueira Jorge[14].

> 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 à distinção entre crimes cibernéticos puros/próprios ou impuros/impróprios, tendo o autor do crime como agente ativo, popularmente conhecido como hacker ou cracker, e qualquer pessoa física ou jurídica ou uma

[13] BRASIL. **Lei 12.737, de 30 nov. 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2012/lei/l12737.htm . Acesso em: 19 abril. 2023

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

> entidade titular, pública ou privada, que sofra a ação ou sobre quem recaiu tal ação é o agente passivo do crime.[15]

O uso crescente da Tecnologia da Informação e Comunicação (TIC) gerou o surgimento de novas categorias de crimes que se beneficiam da facilidade de acesso e propagação de informações oferecida pela internet. Dentre estes, estão a disseminação de vírus e *malwares*, a invasão de sistemas, o roubo de informações pessoais e financeiras, a espionagem cibernética e o *phishing*, que consiste em enganar usuários para obter suas informações pessoais e financeiras.

Dessa forma, o surgimento desses delitos pode ser creditado à evolução tecnológica e à popularização da internet, assim, a tecnologia da informação, com sua rapidez e flexibilidade, permite ao criminoso uma maior eficiência na realização de suas atividades delituosas, complicando o trabalho das autoridades na repressão e punição desses crimes. Com isso, podemos identificar várias formas de crimes cibernéticos, cada um com suas características específicas: *phishing, ransomware, botnets, malware*, ataque DDoS, *cyberbullying*.[16]

Nesse viés, torna-se relevante a discussão acerca da invasão de privacidade na internet, visto que muitos sites e aplicativos coletam dados pessoais dos usuários, muitas vezes sem o conhecimento dos mesmos, e usam essas informações para fins comerciais.

Sob essa óptica, os crimes cibernéticos têm um impacto econômico significativo, com perdas estimadas em trilhões de dólares anualmente. Eles afetam empresas de todos os setores e governos. Além disso, o uso crescente de criptomoedas, como o Bitcoin, tem facilitado a realização de transações financeiras ilegais na internet. Essas moedas digitais são usadas por criminosos para realizar atividades ilegais, como lavagem de dinheiro, compra e venda de drogas e armas e financiamento do terrorismo.

Para enfrentar esses desafios, é fundamental que empresas, governos e indivíduos adotem medidas de segurança cibernética eficazes. Além disso, é crucial que as autoridades tomem medidas para reprimir e punir os criminosos cibernéticos. Isso inclui a criação de legislações específicas e a cooperação internacional para rastrear e identificar os responsáveis pelos crimes. Afinal, muitos desses delitos são

---

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

[16] RAINS, Tim. **CybersecurityThreats, Malware Trends, andStrategies:** mitigateexploits, malware, phishingandother social engineeringattacks. Birmingham: PacktPublishing Ltd, 2020. 429 p.

realizados por criminosos que operam além das fronteiras nacionais, o que dificulta a extradição e a responsabilização.

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), no primeiro semestre de 2021 foram registrados mais de 1,6 milhão de incidentes de segurança na internet no país.[17]

Frente a isso, os crimes cibernéticos podem ser divididos em duas categorias: os crimes cibernéticos propriamente ditos e os crimes cibernéticos impróprios.

Os crimes cibernéticos impróprios envolvem atividades criminosas em que o computador ou a rede de computadores são utilizados como instrumentos para a prática do delito, como na fraude eletrônica, clonagem de cartões de crédito e sequestro de dados. Já os crimes cibernéticos propriamente ditos envolvem atividades criminosas em que o computador ou a rede de computadores é o objeto do delito, como o acesso não autorizado a sistemas, a disseminação de vírus e malware e a sabotagem de sistemas de informática.

2.2.1. CRIMES INFORMÁTICOS IMPRÓPRIOS

Crimes informáticos impróprios, ou acessórios, são crimes tradicionais que se aproveitam da tecnologia da informação para sua execução, sem necessariamente ter uma conexão intrínseca com o ambiente virtual. Eles usam a internet como um meio para facilitar ou ocultar a prática do crime, podendo causar sérias consequências para as vítimas. Assim, diferente dos crimes informáticos típicos, esses delitos não exigem conhecimentos técnicos aprofundados em informática ou sistemas de dados. O objetivo desses crimes não é necessariamente violar a segurança dos dados informatizados, mas sim atingir outros bens jurídicos, já protegidos por tipos penais existentes, praticando ações criminosas que ocorrem no cotidiano. Nesse sentido, a conduta do agente se amolda aos tipos penais tradicionais, porém executada por meio de um computador, lesionando bens jurídicos diversos dos informáticos para atingir o resultado pretendido.

---

[17] CERT.br. **Incidentes reportados ao CERT.b**r: Janeiro a Junho de 2020. 2020. Disponível em: https://www.cert.br/stats/incidentes/2020-jan-jun/fraude.html. Acesso em: 18 abr. 2023.

Os crimes informáticos impróprios englobam uma variedade de condutas criminosas, alguns exemplos são[18]:

(i) Fraudes financeiras e estelionato: o agente se vale de práticas enganosas para obter vantagens financeiras indevidas. No ambiente virtual, essas fraudes podem ocorrer por meio de softwares maliciosos, como *keyloggers,* que roubam as senhas bancárias das vítimas, ou por meio de técnicas de engenharia social, como páginas falsas de bancos que solicitam dados pessoais e bancários.

(ii) Clonagem de cartões de crédito: os criminosos utilizam dispositivos para copiar informações dos cartões de crédito das vítimas, realizando compras fraudulentas ou outros tipos de transações financeiras ilegais em seus nomes.

(iii) Sequestro virtual: prática em que os criminosos obtêm acesso a informações pessoais ou arquivos da vítima e exigem um pagamento para liberá-los.

(iv) Invasão de dispositivos eletrônicos: ação em que o criminoso obtém acesso não autorizado a dispositivos de terceiros, como computadores ou smartphones, para obter informações pessoais da vítima que podem ser utilizadas para a prática de crimes financeiros e outros tipos de crimes informáticos.

(v) Divulgação não autorizada de informações pessoais: esta prática criminosa, comum em casos de vazamentos de dados, envolve a exposição de dados sensíveis, como fotos, informações financeiras e outros dados privados na internet.

(vi) Difamação e calúnia: crimes contra a honra, potencializados pela facilidade de disseminação de informações na internet e pelo fato de que muitas vezes a vítima não sabe quem é o autor da ofensa.

(vii) Falsificação de documentos eletrônicos: prática criminosa que envolve a utilização de *softwares* para a falsificação de documentos, como notas fiscais, boletos bancários, contratos e outros documentos.

(viii) Uso indevido de informações pessoais para transações financeiras ilegais: nesse tipo de delito, o criminoso usa dados pessoais de terceiros para efetuar transações financeiras fraudulentas, como a abertura de contas bancárias ou obtenção de empréstimos.

---

[18] ARAS, Vladimir. **Crimes de informática:** Uma nova criminalidade**.** In: Jus Navigandi, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: http://jus.com.br/artigos/2250. Acesso em 14 abr. 2023.

(ix) Espionagem empresarial: prática criminosa em que um indivíduo ou uma empresa coleta informações confidenciais de outras empresas para obter vantagens competitivas.

(x) Sabotagem de sistemas de informática: prática que envolve ações destinadas a prejudicar o funcionamento de sistemas de informática, como servidores e redes de computadores.

(xi) Assédio e perseguição virtual: práticas criminosas em que o agente usa a internet para ameaçar, difamar ou perseguir uma vítima. Esses crimes podem ter sérias consequências psicológicas para as vítimas e necessitam de combate efetivo por parte das autoridades.

Sob essa óptica, segundo Valdir Sznick, professor de direito penal da Universidade de São Paulo, "os crimes informáticos impróprios podem ser caracterizados como crimes tradicionais cometidos com o uso da tecnologia da informação como instrumento ou meio, tendo ou não relação com a própria natureza virtual do objeto da conduta delitiva". Isso inclui desde fraudes financeiras e estelionatos até crimes contra a honra, como difamação e calúnia, cometidos por meio de redes sociais e aplicativos de mensagens.

Um outro exemplo emergente de crime informático impróprio é o chamado "golpe do amor", que tem se tornado cada vez mais comum na internet. Nesse golpe, criminosos criam perfis falsos em sites de relacionamento e aplicativos de namoro, fingindo estar interessados em um relacionamento amoroso. Assim, depois de conquistar a confiança da vítima, os criminosos se aproveitam e solicitam dinheiro ou informações pessoais, como senhas de cartões de crédito e dados bancários. Da mesma forma, em relação à proteção da infância e da adolescência, a pedofilia e a pornografia infantil são crimes gravíssimos que têm sido potencializados pela internet, mesmo diante do Estatuto da Criança e do Adolescente (ECA), que prevê punições rigorosas para tais condutas.

Além disso, crimes de ódio, como o racismo, e crimes graves, como o terrorismo, também podem ser realizados ou potencializados através da internet. Ambos são punidos por legislação específica e representam uma ameaça significativa à sociedade.

Contudo, apesar de os bens jurídicos visados nesses tipos de crimes já estarem protegidos pelo ordenamento jurídico atual, com as respectivas condutas atentatórias tipificadas, isso não exclui a necessidade de os delitos clássicos,

quando praticados por instrumentos informáticos e a partir do espaço virtual, receberem uma tipificação própria e adequada às suas peculiaridades, isso visa garantir um efetivo exercício da jurisdição, limitando a necessidade de usar analogias para enquadrar essas condutas tendo em vista que há uma série de crimes bastante comuns na internet, onde o anonimato e a grande circulação de informações podem facilitar a propagação de ofensas e falsidades.

Diante disso, a dificuldade de investigação e repressão dos crimes informáticos impróprios se deve à sua natureza multifacetada e ao uso de técnicas sofisticadas para ocultar a autoria dos delitos. Além disso, muitas vezes as vítimas não percebem que foram enganadas ou não têm conhecimento dos seus direitos, o que dificulta a identificação e punição dos criminosos.[19] Como explica Damásio de Jesus, 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.[20]

Diante deste cenário, é evidente que o computador e a internet não são apenas ferramentas de conveniência e produtividade, mas também meios para a prática de atividades ilícitas. Assim, devido à falta de proteção e segurança na rede, esses tipos de crimes representam um grande desafio para a segurança cibernética em todo o mundo, posto que em muitos casos, essas atividades são variantes digitais de crimes tradicionais, cujas formas de execução foram adaptadas para o ambiente online. Logo, mostra-se fundamental que haja uma compreensão clara desses crimes e de suas variantes digitais, bem como estratégias eficazes de prevenção, detecção e resposta. A legislação deve acompanhar a evolução da tecnologia, e os usuários devem estar cientes dos riscos associados ao uso da internet, a fim de se protegerem e contribuírem para um ambiente online mais seguro.

---

[19] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos:** dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. Disponível em https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios da-autoria-e-prova-da-materialidade. Acesso 05. mai. 2023

[20] JESUS, Damásio de. ARAS, Vladmir. **Crimes de informática**: Uma nova criminalidade. Disponível em .https://jus.com.br/artigos/2250/crimes-de-informática. Acesso em 17 de abril. 2023

2.2.2. CRIMES INFORMÁTICOS PRÓPRIOS

Diferentemente dos crimes informáticos impróprios, que já existiam antes da revolução tecnológica e apenas foram adaptados para o contexto digital, existem os denominados crimes informáticos próprios ou puros. Esses tipos de crimes surgiram como resultado direto da digitalização e informatização de dados, sendo exclusivos do universo digital. Assim, são definidos por sua singularidade, distanciando-se dos crimes impróprios, tendo em vista que não possuem um equivalente direto no mundo físico. Logo, com a crescente dependência da sociedade aos sistemas de informática, evidencia-se que os criminosos encontraram novas oportunidades para a prática de crimes e possuem cada vez mais conhecimentos técnicos especializados e avançados na área de computação e processamento de dados, criando novas técnicas de ataque por parte dos criminosos.

Dessa forma, os autores desses crimes, muitas vezes, são indivíduos ou grupos com significativa expertise em tecnologia da informação, capazes de explorar brechas de segurança em sistemas e redes para a execução de suas atividades ilícitas. Tais ataques criminosos cibernéticos visam diretamente aos sistemas de dados, comprometendo a privacidade, a integridade das informações e a acessibilidade, disponibilidade e autenticidade dos dados. Assim, estas ações incluem a criação e disseminação de vírus de computador, invasões de sistemas *(hacking),* no qual é a prática de explorar falhas ou vulnerabilidades em um sistema para obter acesso não autorizado, bem como os ataques de negação de serviço (DoS e DDoS), que são ataques destinados a tornar um serviço ou recurso indisponível. No caso de um ataque DoS, o atacante normalmente sobrecarrega o sistema Além disso há outros atos maliciosos possíveis somente no ambiente digital.

Portanto, estas ações afetam a segurança da informação de maneira ampla, ameaçando a integridade dos sistemas e a confiabilidade das informações armazenadas. Embora menos frequentes, os crimes cibernéticos puros representam uma ameaça particularmente séria, ao ponto que eles necessitam, imperativamente, da utilização do sistema informático não apenas como meio, mas também como o alvo direto da ação criminosa.

Nesses casos, como o próprio sistema de informação é o objetivo central do ataque, no qual implicam agressões diretas ao computador da vítima, permitindo o

acesso não autorizado a dados, senhas e documentos. Isso pode resultar na alteração, inclusão ou destruição dessas informações, comprometendo a integridade e confiabilidade dos sistemas e das informações que eles contêm. Diante disso, acabam requerendo um alto grau de sofisticação técnica e conhecimento profundo dos sistemas de informação, isto torna os crimes cibernéticos puros especialmente desafiadores para a segurança cibernética.

Como leciona o mestre Damásio de Jesus:

> 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.[21]

No âmbito da evolução do cibercrime e da rápida progressão da tecnologia da informação, a legislação frequentemente luta para se manter atualizada em relação às novas formas de conduta prejudicial que surgem no ambiente virtual. Neste cenário, a falta de uma legislação específica e abrangente para regulamentar o cibercrime e punir ações prejudiciais pode resultar em uma lacuna legal. Em tal situação, há ações que, apesar de causarem danos irreparáveis às vítimas, podem não se enquadrar em nenhuma categoria de crime previamente definida pelo Código Penal ou outras leis correlatas. Por isso, são consideradas atípicas e não podem ser punidas de acordo com o princípio da legalidade, também conhecido como reserva legal. Este princípio é uma característica fundamental do sistema jurídico brasileiro, especialmente em matéria penal, e estabelece que ninguém pode ser punido por uma ação que não seja explicitamente considerada um crime por lei.

O princípio da legalidade e o princípio anterioridade da lei penal, com previsão legal no artigo 1º do Código Penal e na CRFB/88 - Constituição Federal de 1988 no artigo 5º, inciso XXXIX, o qual não há crime sem lei anterior que o defina, nem há pena sem prévia cominação legal.

> Em decorrência do princípio da legalidade ou da anterioridade da lei penal, à insuficiência ou a ausência de norma penal tipificando os crimes digitais limita à função punitiva estatal, uma vez que influencia na sensação de insegurança e impunidade, com repercussão negativa para a sociedade brasileira e, em especial, para a comunidade internacional, que há mais de uma década vem

[21] JESUS, Damásio De. ARAS, Vladmir. **Crimes de informática:** Uma nova criminalidade. Disponível em https://jus.com.br/artigos/2250/crimes-de-informatica . Acesso: em 17. abr. 2023.

> chamando à atenção para a necessidade e urgência de controle e prevenção de condutas delituosas no ciberespaço.[22]

Assim, é importante salientar que este cenário traz consigo desafios significativos não apenas para a aplicação da lei, mas também para a proteção dos direitos e liberdades individuais na era digital. A legislação precisa se adaptar para acompanhar a evolução tecnológica e definir claramente os limites da conduta aceitável na internet. Ao mesmo tempo, são necessários para garantir que essas mudanças sejam feitas de maneira a respeitar os direitos fundamentais, como a liberdade de expressão e o direito à privacidade. No mais, torna-se crucial abordar também a necessidade de preparação adequada das autoridades e profissionais da área de segurança cibernética, dado o nível de sofisticação técnico necessário para investigar e combater os delitos informáticos próprios. Isso envolve não apenas a formação técnica, mas também uma compreensão clara das leis e regulamentos relacionados aos crimes cibernéticos.

Diante dessas informações, destaca-se que, de acordo com a doutrina jurídica brasileira, os delitos cibernéticos puros são classificados como crimes formais, de consumação antecipada ou de resultado cortado[23]. Isso significa que a consumação desses crimes ocorre no momento em que a conduta criminosa é executada, independentemente da materialização do resultado no mundo físico.

Ademais, vivifica-se um aspecto preocupante de que muitos criminosos virtuais são motivados pela percepção de impunidade proporcionada pelo ambiente online. Contudo, tanto nos crimes cibernéticos puros quanto nos impróprios, a maioria das atividades na internet deixa rastros digitais. Estes podem, em alguns casos, ser mais evidentes que aqueles deixados por crimes cometidos no mundo físico. Logo, estes vestígios incluem informações registradas durante o acesso às redes de computadores, como os dados do Protocolo de Internet (IP), que é um número identificador único atribuído ao dispositivo ou roteador de internet no momento da conexão, bem como detalhes sobre a localização do dispositivo e dados cadastrais do usuário também podem ser rastreados.

A discussão se enriquece ao considerar que a sofisticação crescente das técnicas de investigação digital tem aprimorado a capacidade das autoridades de

---

[22] WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes Cibernéticos:** Ameaças e procedimentos de investigação. 3 ed. Rio de Janeiro: Brasport, 2021.

[23] SANTOS, Elaine Gomes dos. RIBEIRO, Raisa Duarte da Silva. Restrições à liberdade de expressão e crimes cibernéticos: a tutela penal do discurso de ódio nas redes sociais. **Revista dos Tribunais.** São Paulo: Editora RT. vol. 997. p. 527. ano 2018.

rastrear e identificar autores de crimes cibernéticos. No entanto, ainda enfrentam-se obstáculos significativos, como a necessidade de cooperação internacional, dada a natureza global da internet, e a constante evolução das tecnologias e táticas usadas por criminosos cibernéticos. Além disso, embora a rastreabilidade seja um importante instrumento de investigação e responsabilização, ela levanta questões significativas sobre privacidade e direitos individuais. Portanto, um equilíbrio cuidadoso é necessário para assegurar que medidas de segurança e investigação não infrinjam indevidamente as liberdades civis.[24]

Sob essa óptica, os crimes cibernéticos cobrem uma ampla gama de atividades, todas geralmente realizadas através de uma conexão de rede. Entre as técnicas mais comumente usadas pelos criminosos para a prática dos crimes informáticos propriamente ditos, destacam-se o uso de softwares maliciosos e técnicas de engenharia social para obter informações confidenciais. Além disso, algumas ações ilegais frequentes incluem o acesso não autorizado, a sabotagem, a interceptação de comunicações, fraudes eletrônicas, a disseminação de vírus e malware, difamação e calúnia, e a pornografia infantil.

No Brasil, o crime de invasão de dispositivos informáticos é tipificado pela Lei Carolina Dieckmann[25], podendo levar a até dois anos de detenção e multa. Outro tipo comum de delito digital é a sabotagem, que visa prejudicar ou comprometer a segurança dos sistemas informáticos. Esta ação, geralmente perpetrada através do uso de vírus, *malware, backdoors* e outras técnicas de *hacking,* pode resultar em perda de dados, interrupção de sistemas e prejuízos financeiros. Bem como, à própria disseminação de vírus e *malware*, que se refere à distribuição de programas maliciosos com a intenção direta de danificar os sistemas.

Dentre os crimes próprios, evidencia-se os crimes de difamação e calúnia, que envolvem a propagação de informações falsas ou prejudiciais sobre um indivíduo ou uma empresa, no ambiente digital, sendo ambos tipificados pelo Código Penal brasileiro. No mais, o crime de interceptação de comunicações, que consiste na captação não autorizada de mensagens de texto, áudio, vídeo ou outras

---

[24] SANTOS, Elaine Gomes dos. RIBEIRO, Raisa Duarte da Silva. Restrições à liberdade de expressão e crimes cibernéticos: a tutela penal do discurso de ódio nas redes sociais. **Revista dos Tribunais.** São Paulo: Editora RT.. **v**ol. 997. ano 2018. p. 527.

[25] BRASIL. **Lei 12.737, de 30 nov. 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2012/lei/l12737.htm . Acesso: 19. abril. 2023

formas de comunicação eletrônica, que pode ser realizado através de técnicas de invasão, como a interceptação de pacotes de dados, ou através da instalação de *softwares* maliciosos nos dispositivos dos usuários.

Nessa mesma linha, as fraudes eletrônicas, no qual buscam obter ganhos financeiros ilegítimos através de técnicas de engenharia social, como phishing e spoofing, por meio de envio de mensagens falsas que se passam por comunicações autênticas de empresas conhecidas, como bancos ou lojas online.

Por fim, a pornografia infantil, um crime de extrema gravidade, envolve a produção, distribuição, veiculação ou armazenamento de material pornográfico contendo menores de idade, sendo este delito previsto no Estatuto da Criança e do Adolescente e sujeito a penalidades severas.[26] Sob essa informação, os dados da SaferNet Brasil mostram que, em 2018, o Brasil registrou um total de 133.732 queixas de delitos virtuais, 110% a mais em relação ao ano anterior. O principal crime denunciado foi a pornografia infantil. Segundo a organização, nos últimos 14 anos, mais de 4,1 milhões de denúncias anônimas foram contabilizadas contra 790 mil endereços eletrônicos por divulgarem conteúdo inapropriado na internet. Além desses dados, o jornal New York Times informou, em 2019, que empresas de tecnologia registraram mais de 45 milhões de fotos e vídeos online de crianças vítimas de abuso sexual. O número é mais que o dobro do registrado no ano anterior.[27]

Infere-se pois que o combate a esses crimes deve ser iniciado pelo poder legislativo, juntamente com especialistas em direito digital e cibernético, para que trabalhem na criação e atualização de leis que abordem adequadamente a complexidade do cibercrime. A sociedade precisa ser conscientizada sobre o uso responsável e ético da tecnologia, a fim de minimizar a ocorrência de tais crimes. Os delitos informáticos próprios representam uma ameaça significativa à segurança cibernética, exigindo esforços coordenados entre as forças da lei, especialistas em segurança cibernética e os usuários da internet. Assim, a legislação precisa evoluir para abordar adequadamente esses novos tipos de crime, garantindo que os

---

[26] VALVERDE, Danielle Novaes de Siqueira. Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso. **Revista da ESMAPE.** Recife. v. 15. n. 32. p. 244.

[27] Ministério dos Direitos Humanos e da Cidadania. **Exposição de crianças e adolescentes na internet ocupa 5ª posição no ranking do Disque 100.** Disponível em https://www.gov.br/mdh/pt-br/assuntos/noticias/2020-2/novembro/exposicao-de-criancas-e-adolescentes-na-internet-ocupa-quinta-posicao-no-ranking-de-denuncias-do-disque-100. Acesso: 20 abr. 2023

perpetradores possam ser identificados, processados e punidos de maneira eficaz. Logo, a prevenção, detecção e resposta a esses crimes requerem uma combinação de medidas de segurança robustas, legislação adequada e cooperação internacional[28], além da conscientização dos usuários sobre práticas seguras de uso da tecnologia.

Vale destacar que a prevenção é o aspecto crucial no combate aos crimes digitais. Isso inclui tanto a implementação de medidas técnicas de segurança, como *firewalls* e programas antivírus, quanto a educação e conscientização dos usuários sobre os riscos e as práticas seguras de uso da internet. Afinal, um usuário informado e consciente é um dos melhores antídotos contra o crime cibernético, tornando possível combater eficazmente essa ameaça e garantir a segurança e integridade dos sistemas de informação na era digital.

[28] GUARAGNI, Fábio André. RIOS, Rodrigo Sanchez. **Novas tendências de combate aos crimes cibernéticos: cooperação internacional e perspectivas na realidade brasileira contemporânea**. Revista de Estudos Criminais. Porto Alegre, v. 18, n. 73. p. 181. 2019.

3. O HISTÓRICO E A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS NAS NORMAS NACIONAIS

O advento das tecnologias digitais e da internet trouxe consigo uma nova categoria de crimes, os chamados crimes cibernéticos, que são ilícitos praticados no ambiente digital. A legislação brasileira vem sofrendo adaptações para atender a essas inéditas modalidades de crime, buscando oferecer uma resposta precisa e efetiva à crescente onda de criminalidade cibernética.

No Brasil, até o ano de 2012, não havia uma legislação específica que punisse crimes cibernéticos próprios - ilícitos que só podem ser praticados por meio de um computador ou outros dispositivos tecnológicos. No entanto, houve uma sequência de projetos de lei no Congresso Nacional buscando estabelecer um marco legal para crimes cibernéticos. O primeiro foi o Projeto de Lei nº 84/99, proposto pelo deputado Luiz Piauhylino, também conhecido como Lei dos Crimes Digitais, visando tipificar como crime ações como invasão e modificação de conteúdo de sites, roubo de senhas, criação e disseminação de vírus, dentre outros. Em seguida, o senador Luiz Estevão apresentou o Projeto de Lei do Senado n.º 151/00, propondo a obrigatoriedade da guarda dos registros de conexão dos usuários da internet, uma medida que visava aumentar o controle sobre as atividades online e facilitar a investigação de crimes cibernéticos. A Lei dos Crimes Digitais foi aprovada na Câmara em 2003 e, em 2008, passou por modificações no Senado, retornando à casa de origem para avaliação das alterações propostas.

Em 2011, o Poder Executivo propôs o PL n.º 2.126/11, mais conhecido como Marco Civil da Internet[29], que, em vez de focar nos aspectos penais do uso da internet, assegurava liberdades e direitos aos usuários. Esse projeto buscou regular a rede no âmbito civil, considerado necessário antes de um marco regulatório criminal. Por conseguinte, somente em 2012, após o caso de violação de privacidade envolvendo a atriz Carolina Dieckmann, o Projeto de Crimes Digitais foi aprovado, resultando na Lei nº 12.735/12, também chamada de Lei Azeredo. Contudo, esta nova lei foi drasticamente simplificada e os novos tipos penais foram incorporados à Lei Carolina Dieckmann.

---

[29] BRASIL**. Marco civil da internet:** Lei n. 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 2. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2015.

No que se refere aos crimes cibernéticos impróprios, a maior parte já está tipificada no Código Penal brasileiro. Conforme explicado no item 1.2 deste documento, os crimes cibernéticos impróprios correspondem aos "crimes tradicionais" em que o bem jurídico não é o dado informático em si, sendo a informática utilizada apenas como meio para a prática do delito.

Apesar dos notáveis avanços legislativos no combate aos cibercrimes no Brasil, a legislação nacional ainda se encontra aquém do necessário para a devida regulamentação do uso do ambiente virtual e suas plataformas, além da repressão aos crescentes crimes virtuais em suas vertentes próprias e impróprias. A evolução do ambiente cibernético e as novas modalidades de cibercrimes exigem uma atualização legislativa constante e uma discussão ampla sobre a melhor forma de proteger os direitos dos cidadãos e reprimir atos ilícitos no espaço digital.

Este capítulo segue com a análise da adequação dos principais ataques cibernéticos, conforme descritos no Capítulo I, à legislação brasileira e como estes se alinham às exigências da Convenção de Budapeste. Primeiramente, será feita uma avaliação do cenário jurídico brasileiro em relação ao ambiente cibernético. Em seguida, será analisado se os principais ataques cibernéticos já estão tipificados no ordenamento jurídico nacional e quais medidas legislativas serão necessárias para adequar as leis nacionais aos requisitos estabelecidos pela Convenção de Budapeste.

3.1. LEI Nº 10.695, DE 01 DE JULHO DE 2003

A Lei nº 10.69529, promulgada em 01 de julho de 2003, trouxe modificações significativas ao Código Penal e ao Código de Processo Penal no que tange aos delitos associados à violação de direito autoral e dos direitos conexos. Antes da promulgação desta lei, a legislação brasileira tipificava como crime somente a violação aos direitos de autor, negligenciando os direitos vinculados aos artistas intérpretes ou executantes, produtores fonográficos e empresas de radiodifusão[30]. No mais, o primeiro artigo desta lei promove alterações no artigo 184 do Código Penal, determinando que, no caso de a violação consistir na distribuição, sem fins

[30]CARBONI, Guilherme C. **A Lei nº 10.695/03 e seu impacto no Direito Autoral Brasileiro.** 2003. Disponível em: https://www.migalhas.com.br/depeso/2651/a-lei-n--10-695-03-e-seuimpacto-no-direito-autoral-brasileiro. Acesso: 25 mai. 2023.

lucrativos, de obras intelectuais, fonogramas e videofonogramas reproduzidos com violação do direito de autor, o infrator estará sujeito à pena de detenção de seis meses a dois anos ou multa.

Além de estender a proteção aos direitos conexos, adiciona, por meio de seu parágrafo terceiro, as ações realizadas com suporte tecnológico, visando, primordialmente, o combate à ciberpirataria,[31] incluindo a apreensão de cópias ou reproduções realizadas com violação aos direitos autorais e conexos e a possibilidade de destruição dessas cópias, bem como a possibilidade de interdição de estabelecimentos que cometem esses delitos.

> Art. 184. Infringir direitos de autor e aqueles a ele associados:
>
> ...
>
> § 3o Se a infração consistir em disponibilizar ao público, via cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário escolher a obra ou produção para recebê-la em um tempo e lugar preestabelecidos por quem faz a solicitação, com objetivo de lucro, direto ou indireto, sem a devida autorização, conforme apropriado, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente.

Ao comparar com a Convenção de Budapeste, constata-se que a salvaguarda dos direitos conexos está alinhada ao estabelecido no artigo 10 da referida Convenção. Adicionalmente, a inclusão no ordenamento jurídico brasileiro do terceiro parágrafo do artigo 184 atende ao mandato da Convenção no que se refere à perpetração do delito por intermédio de um sistema informático.

3.2. LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012

A Lei nº 12.735/2012, conhecida como Lei Azeredo, representa um marco relevante no combate aos crimes cibernéticos no Brasil, ao ponto que foi proposta pelo Senador Eduardo Azeredo, sucedendo os projetos de lei nº 89/2003, nº 76/2000 e 137/2000, e sancionada em 30 de novembro de 2012[32]. Essa legislação teve como objetivo primordial tipificar condutas executadas por meio de sistemas eletrônicos digitais, ou similares, e aquelas perpetradas contra sistemas informatizados e seus equivalentes. Nesse viés, os primeiros artigos da Lei

---

[31]GIACCHETTA, André Zonaro. **A nova arma no combate à pirataria - a Lei Nº 10.695, de 2.7.**2003. Migalhas, 2003. Disponível em: https://www.migalhas.com.br/depeso/2275/a-novaarma-no-combate-a-pirataria---a-lei--n---10-695---de-2-7-2003. Acesso em: 25 mai. 2023.

[32] NASCIMENTO, Talles Leandro Ramo**s. Crimes cibernéticos:** Conteúdo Jurídico. Disponível em . https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em 23 mai. 2023

n.º12.735/2012[33] tratam da tipificação de delitos praticados no ambiente virtual, as condutas relacionadas à falsificação de cartão de crédito e ao delito em favor do inimigo, já previstas no Código Penal e no Código Penal Militar, respectivamente, foram inicialmente contempladas nos artigos 2º e 3º, porém vedadas na sanção final da lei. Bem como, contemplou aspectos processuais e penais na luta contra os crimes digitais, conforme o artigo 4º[34], no qual fundamentou a criação de órgãos especializados nesse combate, tendo em vista que a investigação desses delitos geralmente inicia com a localização e manuseio de equipamentos informáticos e dos dados ali armazenados, demandando assim profissionais tecnicamente preparados.

O artigo 5º, por sua vez, modificou a redação do §3º do Art. 20 da Lei n.º 7.716/1989, que define crimes resultantes de preconceito de raça ou de cor, visando coibir a disseminação do preconceito e da intolerância racial por meio das novas tecnologias.

Infere-se que a origem da Lei Azeredo remonta ao Projeto de Lei nº 84/1999, que almejava definir os crimes cibernéticos, tornando certas condutas praticadas nesse ambiente cibernético passíveis de prisão e multa. O projeto inicial foi, por vezes, taxado de "AI-5 Digital", devido à amplitude e rigidez de suas propostas, fator que o deixou em espera por alguns anos[35]. A discussão foi retomada pelo deputado Eduardo Azeredo em 2008 e, após significativas mudanças e a retirada de uma série de artigos, a Lei n.º 12.735/2012 foi finalmente promulgada em 2012, ainda que tenha sofrido veto parcial da então presidente Dilma Rousseff. Embora a Lei Azeredo tenha sido criada especificamente para tipificar os crimes cibernéticos, este papel acabou sendo delegado à Lei n.º12.737 de 2012[36], promulgada no mesmo ano. Dessa forma, a Lei Azeredo desempenhou um papel importante na evolução da legislação brasileira de crimes cibernéticos, estabelecendo as bases para a construção da legislação subsequente.

---

[33] BRASIL. **Lei 12.735, de 30 nov. 2012.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso. 06. jun. 2023.

[34] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos:** Conteúdo Jurídico. Disponível em . https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em 10. mai. 2023

[35] MILAGRE, José Antônio. Lei Azeredo, AI-5 digital e a cultura do contra. Uma visão pessoal sobre o manifesto contra a Lei de Crimes de Informática**. Revista Jus Navigandi,** ISSN 1518-4862, Teresina, ano 14, n. 2216, 26 jul. 2009. Disponível em: https://jus.com.br/artigos/13211. Acesso. 17. mai. 2023

[36] NASCIMENTO, Talles Leandro Ramos. Crimes cibernéticos. Conteúdo Jurídico. Disponível em . https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso 10. mai. 2023

3.3. LEI N.º 12.737, DE 30 DE NOVEMBRO DE 2012

O projeto da Lei n.º 12.737/2012[37] foi apresentado pelo Deputado Federal Paulo Teixeira e promulgado em 30 de novembro de 2012, seguindo um processo acelerado devido à pressão da mídia para uma rápida regulamentação dos crimes virtuais. Esse senso de urgência decorreu do caso da atriz Carolina Dieckmann, cujas fotos íntimas foram distribuídas na internet após a invasão e subtração de conteúdo de sua conta de e-mail por cibercriminosos.[38] Esse incidente deu à lei o apelido popular de "Lei Carolina Dieckmann" e foi reconhecido como um grande avanço legislativo no tema.

A Lei nº 12.737/2012 inovou o ordenamento jurídico brasileiro ao tipificar novos delitos, expandindo a legislação sobre crimes virtuais, introduzindo no Código Penal artigos que tratam da invasão de dispositivo informático, interrupção ou perturbação de serviço telemático ou de informação de utilidade pública e a falsificação de cartão.

Um dos aspectos mais notáveis da Lei é o seu artigo 2º, que tipifica as condutas relativas à "invasão de dispositivo informático". Esse artigo ampliou o Código Penal brasileiro, inserindo os artigos 154-A e 154-B, que visam penalizar a conduta daqueles que invadem, adulteram ou destroem a privacidade digital de terceiros, violando mecanismos de segurança. Entretanto, a lei expressa a necessidade de um mecanismo de segurança no sistema do dispositivo eletrônico da vítima para que a conduta seja considerada crime.

Nessa ótica, o artigo 154-A do Código Penal, incluído pela Lei n.º 12.737/2012, direciona a legislação para combater condutas criminosas baseadas na invasão de dispositivos informáticos de terceiros, conectados ou não à internet, condicionando a criminalização à violação concreta e indevida de mecanismos de segurança. Este artigo também se preocupa com os efeitos patrimoniais da invasão. O artigo 154-B, por outro lado, estabelece que a ação penal para o crime de "invasão de dispositivo informático" será pública, condicionada à representação da

---

[37] BRASIL. **Lei 12.737, de 30 nov. 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2012/lei/l12737.htm . Acesso: 19. mai. 2023

[38] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos:** dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. Disponível em https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios da-autoria-e-prova-da-materialidade. Acesso: 15. mai. 2023

vítima, exceto nos casos em que o delito for cometido contra a administração pública direta ou indireta.[39]

Essas mudanças têm uma correlação com a Convenção de Budapeste. O artigo 154-A *caput* da Lei nº 12.737, por exemplo, está alinhado com o artigo 2º da Convenção, que trata de acesso ilegítimo. Além disso, o parágrafo 1º do artigo 154-A está parcialmente em conformidade com o item 1.a.i do artigo 6 da Convenção, que trata do uso abusivo de dispositivos.

Por conseguinte, a Lei n.º 12.737/2012 também alterou os delitos tipificados nos artigos 266 e 298 do Código Penal. No artigo 266, foi incluído o serviço informático, telemático ou de informação de utilidade pública, tornando sua interrupção um crime. No artigo 298, foi incluído o delito de falsificação de cartão.[40]

Em suma, a criação da Lei Carolina Dieckmann, visou preencher a lacuna normativa existente, objetivando a repressão e punição mais efetiva dos ilícitos praticados no ambiente virtual. Assim, foi um grande passo na modernização da legislação brasileira para lidar com a crescente ameaça dos crimes cibernéticos. No entanto, apesar das melhorias trazidas por essa lei, o combate a esses tipos de crimes ainda apresenta grandes desafios, uma vez que a evolução tecnológica e a globalização tornam o ambiente virtual um campo fértil para a atuação de criminosos.

3.4. LEI Nº 12.965, DE 23 DE ABRIL DE 2014

Antes da implementação do Marco Civil da Internet, o Brasil não possuía uma legislação que abordasse de forma abrangente a questão da internet. Dessa forma, havia apenas resoluções editadas pelo Poder Executivo tentando preencher a lacuna legislativa relativa a questões jurídicas surgidas no ambiente virtual e no uso de suas plataformas. A proposta de lei que levou à criação da Lei n.º 12.965/2014 começou em 2009 com a apresentação do projeto de lei n.º 2.126/2011. O texto do projeto de lei foi submetido à consulta pública em várias cidades do país, com várias sugestões relacionadas ao tema sendo discutidas pelo Legislativo e muitas delas incorporadas ao texto final.

---

[39] NASCIMENTO, Talles Leandro Ramos. **Crimes cibernético**s. Conteúdo Jurídico. Disponível em . https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso: 16. mai. 2023

[40] NASCIMENTO, Talles Leandro Ramos. Crimes cibernéticos. Conteúdo Jurídico. Disponível em . https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso: 16. mai. 2023

Com isso, o Marco Civil da Internet é a designação dada à Lei n.º 12.965, promulgada em 23 de abril de 2014[41]. Desenvolvido pelo Ministério da Justiça, o projeto de lei estabelece diretrizes, princípios, garantias, direitos e deveres para o uso da internet no Brasil, aplicáveis a usuários, governo e provedores de serviços e acessos. A lei foi concebida com o objetivo de promover o uso ético da internet, consolidando os direitos dos usuários, especialmente à inviolabilidade da intimidade e da vida privada, embora não tenha tipificado nenhuma conduta.[42]

Por conseguinte, a lei é especialmente cuidadosa com a questão da liberdade de expressão e a proibição da censura. O artigo 2º e o artigo 19 garantem expressamente esses direitos. Da mesma forma, o artigo 3º, I, estabelece como princípios do uso da internet no Brasil a liberdade de expressão, comunicação e manifestação do pensamento. A Lei n.º 12.965/2014 também destaca a importância da privacidade, garantindo aos usuários da internet a inviolabilidade da intimidade e vida privada, a preservação do sigilo das comunicações transmitidas ou armazenadas, e a não divulgação de dados coletados pela internet sem o prévio consentimento do usuário.[43]

A questão do registro e guarda dos *logs* de acesso dos usuários à rede também é abordada no Marco Civil da Internet. O artigo 14 estabelece que os provedores de acesso e conteúdo na internet não podem guardar registros de acesso sem o prévio consentimento do usuário. O artigo 13 impõe a obrigação de guarda dos registros de acesso dos usuários pelo período mínimo de um ano.

Nesse viés, também estabelece regras para a responsabilidade civil dos provedores de internet em caso de ofensa aos direitos da personalidade das pessoas[44]. Assim, os provedores podem ser responsabilizados, por exemplo, por danos decorrentes de conteúdos publicados em suas plataformas caso não os removam após ordem judicial. Bem como, o artigo 29 e seu parágrafo único estabelecem o direito do usuário da internet de instalar em seu computador pessoal

---

[41] BRASIL. **Marco civil da internet:** Lei n. 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 2. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2015.

[42] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos**: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. Disponível em https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indiciosda-autoria-e-prova-da-materialidade. Acesso: 05 mai. 2023

[43] NASCIMENTO, Talles Leandro Ramos. Crimes cibernéticos. Conteúdo Jurídico. Disponível em . https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso: 16 mai. 2023

[44] BITTAR, Carlos Alberto. **Os Direitos da Personalidade.** Rio de Janeiro: Forense Universitária, 1989.

programas destinados ao controle parental, ou seja, do conteúdo entendido como impróprio para filhos menores. Logo, o Marco Civil da Internet funciona como uma espécie de Constituição da internet, estabelecendo os direitos e deveres dos usuários da rede, dos provedores de acesso e de conteúdo, bem como do próprio Estado.

No entanto, a proteção que deveria ser oferecida pela lei penal ainda não foi totalmente efetivada. A inviolabilidade da intimidade, e da vida privada e, a inviolabilidade do sigilo do fluxo de comunicações ainda são tratadas apenas no artigo 7º da lei. Todavia, de forma semelhante, a Lei de Proteção de Dados, Lei n.º 13.709, que regulamenta o Marco Civil da Internet, ainda não atende às necessidades de inovações legislativas para a proteção de bens jurídicos por meio de normas criminais.[45]

Infere-se que o Marco Civil da Internet, representa um marco significativo na legislação brasileira ao estabelecer diretrizes, princípios, direitos e deveres para o uso da internet no país, importantes para os usuários da internet, como a liberdade de expressão, a inviolabilidade da intimidade e da vida privada e o sigilo das comunicações. Além disso, estabelece as bases para a responsabilidade civil dos provedores de internet em casos de ofensa aos direitos da personalidade das pessoas. Embora represente um progresso importante, a aplicação integral do Marco Civil da Internet ainda enfrenta desafios. A proteção jurídica que deveria ser garantida pela legislação penal ainda não está totalmente efetivada, o que abre espaço para debates contínuos sobre como fortalecer a proteção dos direitos do usuário na era digital. Logo, mostra-se como uma lei pioneira que busca equilibrar a liberdade de expressão e os direitos de privacidade dos usuários na internet com a necessidade de regular o uso da internet e proteger os direitos individuais, posto que seu impacto completo ainda está sendo avaliado e sua efetivação completa ainda é um desafio.

3.5 LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

A relevância da proteção de dados se amplia à medida que nosso mundo se torna cada vez mais digital, onde os dados pessoais emergem como ativos

[45] GUARAGNI, Fábio André. RIOS, Rodrigo Sanchez. **Novas tendências de combate aos crimes cibernéticos:** cooperação internacional e perspectivas na realidade brasileira contemporânea. Revista de Estudos Criminais. Porto Alegre, v. 18, n. 73. p. 181, 2019.

inestimáveis para várias empresas e organizações. Em ambos os contextos, o brasileiro e o global, a implementação de leis e regulamentos robustos busca salvaguardar a privacidade dos cidadãos, estabelecendo diretrizes claras para as entidades que manipulam essas informações. A ascensão dessa nova configuração social, apoiada em grande parte na ubiquidade da internet, remodelou nossas interações, economias e a forma como nos relacionamos com o conhecimento e a informação. Contudo, junto a essas inúmeras possibilidades de crescimento e transformação, a sociedade conectada se apresenta como um ambiente propício ao surgimento e proliferação do cibercrime. Este capítulo explora o desenvolvimento e a proteção dos dados frente aos cibercrimes.

No Brasil, temos a Lei Geral de Proteção de Dados (LGPD)[46], sancionada em 2018 e efetivamente aplicada desde setembro de 2020. Assim, mostra-se como uma legislação inovadora no Brasil, estabelecendo princípios e conceitos direcionadores para um uso seguro de dados. Esta lei tem como objetivo equilibrar a proteção eficaz dos direitos dos titulares desses dados e, simultaneamente, permitir o processamento de dados pessoais e sensíveis para propósitos específicos, incluindo a pesquisa científica. A LGPD introduziu pela primeira vez no sistema jurídico brasileiro um conjunto de normas e princípios voltados para a regulação do tratamento de dados pessoais em todas as atividades diárias dos cidadãos, abrangendo vários setores.

Neste contexto contemporâneo, quase todas as relações humanas ocorrem no mundo online, seja na compra de produtos, na atividade profissional, na busca por educação e conhecimento, ou no cumprimento de obrigações legais como a declaração de imposto de renda. Vida cotidiana e interações humanas estão sempre gerando e compartilhando enormes quantidades de dados por meio de várias ferramentas digitais.

Nesse sentido, o artigo 2º da Lei Geral de Proteção de Dados[47], elenca os princípios fundamentais da proteção de dados pessoais: respeito à privacidade, autodeterminação informativa, liberdade de expressão, inviolabilidade da intimidade, honra e imagem, bem como o desenvolvimento econômico, tecnológico e a

---

[46] BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm; Acesso: 27 mai. 2023

[47] BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm; Acesso: 27 mai. 2023

inovação, entre outros. Esta complexa intersecção de privacidade, direitos humanos, liberdade, dignidade e desenvolvimento econômico aponta para a dualidade da legislação: ao mesmo tempo em que protege a privacidade do indivíduo, também promove o crescimento econômico e tecnológico. O contexto atual de constante exposição nas redes sociais, seja por escolha pessoal ou necessidade profissional, traz novos desafios para a proteção de dados.

O artigo 3º da LGPD estabelece que a lei será aplicada independentemente do meio, do país da sede ou de onde os dados estão localizados. No entanto, existem exceções à aplicação desta lei, como no caso do tratamento de dados por indivíduos para fins exclusivamente privados, uso para finalidades jornalísticas, artísticas ou acadêmicas, ou para segurança pública, defesa nacional e investigação criminal, entre outros. A LGPD também define termos-chave como "dados pessoais" e "dados sensíveis". Estes últimos são particularmente importantes para a privacidade, pois uma violação pode resultar em consequências graves. Uma maior proteção é concedida a esses dados, que estão intrinsecamente ligados à liberdade e à dignidade do indivíduo.

Assim sendo, a lei também estipula diretrizes para o tratamento de dados pessoais, incluindo princípios como boa-fé, finalidade, adequação, necessidade e livre acesso. Além disso, a lei destaca a qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização. No último ponto, espera-se que as medidas adotadas para a proteção de dados pessoais sejam eficazes e possam demonstrar o cumprimento das normas de proteção de dados. O artigo 7º da LGPD apresenta uma série de cenários para o tratamento de dados, enfatizando a necessidade de consentimento do titular e o direito à autodeterminação informativa. Além disso, aborda o tratamento de dados pela administração pública e por órgãos de pesquisa, sempre buscando, quando possível, a anonimização dos dados pessoais.

Dessa forma, a LGPD[48] é a principal legislação que rege a proteção de dados pessoais, bem como traça paralelos com o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia[49]. Estabelece regras rígidas e abrangentes que

[48] BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm; Acesso: 27 mai. 2023

[49] COMISSÃO EUROPEIA. **Proteção de dados nas instituições e outros organismos da UE.** Disponível em https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt#:~:text=O%20Regul

todas as empresas precisam aderir ao lidar com coleta, armazenamento, processamento e compartilhamento de dados pessoais. Além disso, dá maior atenção à proteção de dados sensíveis, como informações de saúde ou dados biométricos.

A implementação no Brasil tem sido um desafio tanto para as organizações, quanto para os órgãos de fiscalização. Muitas empresas tiveram que se adaptar às exigências da lei, reavaliando suas práticas de coleta, armazenamento e tratamento de dados. A adequação à LGPD envolve a implementação de medidas de segurança adequadas, a revisão de políticas de privacidade, a realização de auditorias internas e a capacitação dos colaboradores para garantir o cumprimento das disposições legais.

Internacionalmente, a proteção de dados no espaço digital é um tópico de destaque em debates e elaboração de leis. O GDPR da União Europeia é frequentemente referenciado como uma norma na proteção de dados, com ênfase em princípios como minimização de dados, transparência, integridade e confidencialidade de dados, e a abordagem de "privacidade desde o design". Países como Austrália, Canadá e Japão também possuem leis de proteção de dados, sinalizando a crescente importância desse tema.

A digitalização trouxe desafios singulares para a proteção de dados. A disseminação das redes sociais e o surgimento da Internet das Coisas *(IoT)* ampliaram a quantidade de dados pessoais coletados e processados. Ademais, o avanço do aprendizado de máquina e da inteligência artificial permite análises mais refinadas desses dados, ampliando as preocupações com privacidade.

Para enfrentar tais desafios, é primordial o consentimento informado. As empresas devem garantir que os indivíduos compreendam como e por que seus dados serão utilizados antes de coletá-los. Além disso, é crucial que as empresas adotem as melhores práticas em segurança de dados, como a criptografia e anonimização de dados, para proteger os dados pessoais contra vazamentos e usos indevidos.

A proteção de dados no Brasil e no mundo digital é uma questão de vital importância, dada a crescente coleta e processamento de dados pessoais. Assim,

---

amento%20(UE)%202018%2F,Dados%20na%20Aplica%C3%A7%C3%A3o%20da%20Lei. Acesso: 28 mai.2023

apesar dos avanços significativos proporcionados pela LGPD[50], a proteção de dados no Brasil ainda enfrenta desafios. A efetiva implementação da lei depende não só da conscientização dos cidadãos sobre seus direitos, mas também do comprometimento das empresas em cumprir as regulamentações. Além disso, é necessário que o Estado atue de forma diligente para garantir o cumprimento da lei.

Portanto, a proteção de dados no Brasil é um campo em evolução, que demanda uma atenção contínua para garantir que os direitos dos indivíduos sejam respeitados na era digital. A LGPD é um passo importante nessa direção, mas a realização plena de seus objetivos requer a colaboração de todos os envolvidos, desde os cidadãos até as empresas e o Estado. Logo, à medida que a legislação continua a evoluir para acompanhar as mudanças tecnológicas, a conscientização e o cumprimento dessas leis se tornarão cada vez mais críticos para garantir a privacidade e a proteção dos direitos dos indivíduos, frente ao anonimato notoriamente prejudicial.

3.6. LEI Nº 13.964, DE 24 DE DEZEMBRO DE 2019

A Lei n.º 13.964[51], conhecida amplamente como Lei Anticrime, foi promulgada no dia 24 de dezembro de 2019, proporcionando uma extensa gama de modificações[52] no sistema jurídico penal brasileiro, especialmente no Código Penal, no Código de Processo Penal, na Lei de Execução Penal e em outras legislações específicas.[53]

Dessa forma, a criação do "juiz de garantias" é uma das inovações mais salientes desta lei. Este novo papel foi criado para atuar na etapa do inquérito policial, sendo responsável pela análise de pedidos como a quebra de sigilo ou a emissão de mandados de prisão preventiva, visando garantir maior imparcialidade na fase de julgamento. Outro aspecto notável da Lei Anticrime é a implementação

---

[50] BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm; Acesso em 27.mai.2023

[51] BRASIL. **Lei nº 13.964 de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso: 25 jan. 2022.

[52] CUNHA, Rogério Sanches. Pacote Anticrime: Lei n. 13.964/19 - **Comentários às alterações no CP, CPP e LEP.** Salvador: Juspodivm, 2020b.

[53] CARDOSO, Luiz Eduardo; FALAVIGNO, Chiavelli Facenda. **Do Pacote Anticrime ao Código Penal**: uma análise comparativa da disciplina da perda alargada na Lei n. 13.964/2019. 2020. No prelo.

do Acordo de Não Persecução Penal (ANPP)[54]. Esta medida concede ao Ministério Público a possibilidade de propor um acordo ao acusado em casos de crimes sem violência ou grave ameaça, com pena mínima inferior a 4 anos.

Nesse viés, evidencia-se que houve também uma introdução de maior rigidez na progressão de regime para condenados por crimes hediondos e ampliou o conceito de legítima defesa para incluir agentes de segurança pública. Além disso, modificou as regras para o cumprimento de pena, estipulando que o condenado só será considerado apto para a progressão de regime após cumprir 40% da pena, caso seja reincidente, ou 25%, se for primário.

No contexto de combate ao crime organizado, a Lei Anticrime aprimorou o uso de instrumentos como as colaborações premiadas e a infiltração de agentes, além de endurecer a legislação em relação às organizações criminosas. Em termos de alterações legislativas, a Lei também modificou a Lei nº 9.296/96, que regulamenta as interceptações telefônicas.[55]

Diante disso, a lei introduziu o artigo 10-A, que tipifica a prática de realizar captação ambiental de sinais eletromagnéticos, ópticos ou acústicos para fins de investigação ou instrução criminal sem a devida autorização judicial. Desta maneira, representa um marco importante na legislação penal brasileira, introduzindo diversas mudanças destinadas a aprimorar a justiça penal e proporcionar um combate mais eficiente à criminalidade. Contudo, é importante destacar que certos aspectos desta lei têm gerado intensos debates na comunidade jurídica e na sociedade em geral, sinalizando que a aplicação e a efetividade continuarão a ser alvo de análises e discussões no futuro.

Embora essa nova tipificação criminal esteja em conformidade com as disposições do artigo 3º da Convenção de Budapeste, é importante notar que o crime só ocorre quando a captação de sinais é feita com o objetivo específico de investigação ou instrução criminal. Isso significa que outras formas de captação de sinais, que não estejam relacionadas à investigação ou instrução criminal, não são consideradas crimes sob esta lei.

---

[54]SENADO FEDERAL. **Projeto de Lei n. 6.341, de 2019.** 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/140099.

[55] LIMA, Renato Brasileiro de. **Pacote Anticrime:** Comentários à Lei 13.964/2019. Disponível em: https://www.cnmp.mp.br/portal/images/Publicacoes/documentos/2021/Pacote_Anticrime_volume_2.pdf. artigo por artigo. Salvador: Juspodivm, 2020. Acesso: 29.maio.2023

3.7 LEI Nº 14.155, DE 27 DE MAIO DE 2021

A Lei n.º 14.155[56], sancionada em 27 de maio de 2021 no Brasil, introduziu uma série de mudanças substanciais na legislação penal e processual penal, com um foco específico em crimes realizados através da internet. Assim, a lei buscou elevar a pena para o crime de invasão de dispositivo informático, conforme definido no artigo 154-A do Código Penal, além de ampliar o escopo do delito, removendo a exigência de que a invasão ocorra mediante violação de mecanismo de segurança.

> 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. ...
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.

No artigo 155 do Código Penal, referente ao crime de furto qualificado, a lei introduz alterações que aumentam a pena quando o furto é cometido através de fraude eletrônica ou com o uso de programa malicioso, particularmente se a vítima for idosa ou vulnerável. No contexto do crime de estelionato, detalhado no artigo 171 do Código Penal, a lei inaugura o "estelionato eletrônico", caracterizado pela utilização de informações fornecidas pela vítima ou por terceiros induzidos ao erro por meio de redes sociais, contatos telefônicos ou envio de e-mail fraudulento. A lei também prevê aumento de pena para crimes realizados utilizando um servidor mantido fora do território nacional ou quando o delito é cometido contra um idoso ou pessoa vulnerável.

O diálogo em torno da Lei nº 14.555/2021[57] suscita questões relevantes sobre a justiça das penas para crimes digitais. As sanções estabelecidas são rígidas, e em determinados casos, são mais severas do que as de crimes que afetam diretamente a vida ou a saúde das pessoas. Essa incongruência sublinha o desafio enfrentado pelos legisladores ao tentar equilibrar a necessidade de punir e prevenir delitos digitais com o objetivo de manter a consistência do sistema penal.

---

[56]BRASIL.**Lei 14.155, de 27 de maio de 2021**. Aperfeiçoa a legislação penal e processual penal. Disponível emhttp://https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso: 01.jun.2023

[57]CAVALCANTE. Márcio André Lopes. Lei 14.155/2021: **promove alterações nos crimes de violação de dispositivo informático, furto e estelionato** https://www.dizerodireito.com.br/2021/05/lei-141552021-promove-alteracoes-nos.html. Acesso 3. jun.2023

Todavia, além das modificações na lei, medidas preventivas e educativas são fundamentais na luta contra os crimes digitais. Informar o público sobre os perigos online e incentivar comportamentos seguros na internet são componentes cruciais para minimizar a probabilidade desses crimes. Portanto, as estratégias para combater delitos digitais devem ser extensa, implicando não apenas na implementação rigorosa da lei, mas também na promoção da segurança digital e na educação tecnológica.

Portanto, a Lei nº 14.555/2021 representa um marco importante na legislação penal e processual penal brasileira, introduzindo penalidades mais rígidas e esclarecendo a jurisdição para crimes cometidos eletronicamente. Além disso, a lei expande o escopo de determinados crimes, como a invasão de dispositivos informáticos e o estelionato eletrônico, em resposta às mudanças tecnológicas e sociais que exacerbaram a incidência desses delitos. No entanto, a discussão continua em torno de certos aspectos da lei, como a determinação da jurisdição com base no domicílio da vítima, o que pode representar obstáculos à eficiência da investigação e do processo penal. Continuar a revisão e aprimoramento da legislação é crucial para garantir uma resposta adequada e justa aos crimes cibernéticos, considerando as complexidades inerentes a esses tipos de delitos.

4. A INSUFICIÊNCIA DE LEGISLAÇÃO INTERNA PARA O COMBATE À CIBERCRIMINALIDADE

Nesta era moderna, marcada pela proliferação do espaço digital, assistimos a um processo de globalização acelerada. As inovações tecnológicas, embora ofereçam benefícios incontestáveis, também nos confrontam com desafios novos e complexos, como o surgimento de cibercrimes. Diante deste cenário, este terceiro capítulo de análise pretende examinar as limitações da legislação atual no combate à cibercriminalidade. A complexidade e o anonimato oferecido pela Internet e a criação de obstáculos na localização e punição dos cibercriminosos, propiciando um ambiente de impunidade que estimula a proliferação dos cibercrimes.

Além disso, iremos considerar a Convenção de Budapeste, um instrumento legal internacional criado para padronizar leis nacionais, aumentar as capacidades investigativas e impulsionar a cooperação internacional em matéria de cibercriminalidade.

Finalmente, debateremos a incorporação da Convenção de Budapeste na legislação brasileira e os possíveis impactos desta ação no combate ao cibercrime. Com este capítulo, buscamos fornecer uma visão abrangente do atual estado legislativo em relação à cibercriminalidade, destacando as brechas existentes e propondo possíveis soluções.

O Brasil, classificado pela Organização das Nações Unidas como o quarto país com o maior número de internautas, ilustra essa realidade[58]. Infelizmente, a legislação em vigor e sua aplicação ainda são insuficientes para acompanhar a rapidez e a sofisticação da evolução da cibercriminalidade. Portanto, é essencial que o Direito avance na mesma velocidade que os progressos tecnológicos, especialmente no que diz respeito aos crimes digitais.

Para lidar com a crescente cibercriminalidade e suas peculiaridades, foi fundada em 2005 a Safernet, uma organização não governamental que opera em conjunto com o Ministério Público Federal, desde 2006. Assim, esta instituição recebe, por meio eletrônico, denúncias de crimes cibernéticos, procede à análise

---

[58] SANCHES, Ademir Gasques. ANGELO, Ana Elisa de. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil. Acesso: 28.maio.2023

dessas queixas e, caso se confirme a procedência, encaminhe ao Ministério Público e à Polícia Federal para as devidas ações jurídicas[59].

Nesse mesmo panorama, a nº Lei 12.735/12[60], também conhecida como Lei Azeredo, sancionada como uma resposta necessária ao aumento da cibercriminalidade, de modo a fornecer ao sistema legal brasileiro as ferramentas necessárias para lidar com crimes cibernéticos. No qual, seu principal objetivo foi tipificar condutas cometidas através de sistemas eletrônicos digitais ou similares, ou que sejam realizadas contra sistemas informatizados e equivalentes.

Entre os atos ilícitos que a lei aborda, estão a invasão de dispositivos informáticos para obtenção, adulteração ou destruição de dados ou informações sem a autorização expressa ou tácita do titular do dispositivo, ou a instalação de vulnerabilidades para obter vantagem ilícita. Logo, prescreve que as autoridades judiciárias constituam departamentos especializados no combate aos crimes cibernéticos.

Entretanto, mesmo após longos anos da promulgação desta lei, poucos estados brasileiros efetivaram a implementação de tais departamentos especializados. A expertise é indispensável para lidar efetivamente com a cibercriminalidade, requer conhecimento especializado e a capacidade de se adaptar a um ambiente altamente mutável. Assim, a falta de departamentos especializados dificulta a realização de investigações adequadas desses crimes, muitas vezes resultando em baixas taxas de sucesso e contribuindo para a continuação da impunidade. Portanto, é de suma importância a formação de agentes do estado na área de informática e cibercriminalidade, bem como a criação de setores especializados nas organizações competentes.

Considerando a questão sob esta ótica, percebe-se que a investigação de crimes cibernéticos, apesar de seguir os procedimentos gerais estabelecidos no Código de Processo Penal, requer um conjunto único de competências e recursos, dada a sua peculiaridade. A falta de uma legislação dedicada e que oriente adequadamente a investigação de crimes cibernéticos constitui uma lacuna

---

[59] SAFERNET BRASIL: Protegendo os Direitos Humanos na Sociedade da Informação. **Parcerias com o MPF.** Disponível em https://www.safernet.org.br/site/institucional/parcerias/mpf. Acesso: 01 jun. 2023

[60] BRASIL. **Lei 12.735, de 30 nov. 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, p. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso: 01 jun. 2023

atualmente preocupante, destacando-se que a legislação existente não possui clareza nem abrangência suficientes para combater efetivamente a cibercriminalidade. Logo, a redação ambígua e as definições imprecisas das leis atuais geram insegurança e incertezas jurídicas.

Nesse sentido, o Código Penal brasileiro, cuja criação remonta a 1940[61], se mostra insatisfatório para lidar com muitos comportamentos criminosos atuais, em especial aqueles ligados à cibercriminalidade. Assim sendo, são crimes que normalmente já estão tipificados, mas que são cometidos de maneiras novas e danosas por meio da internet, não encontrando respostas adequadas na legislação vigente. Por isso, o Brasil tem uma necessidade urgente de implementar legislação sólida e especializada que trate especificamente da cibercriminalidade, levando em conta a singularidade desses crimes e se adaptando às suas características em constante mudança. Assim, a formulação dessa legislação deve ser uma prioridade para as autoridades brasileiras.

Neste contexto, a Convenção de Budapeste[62] sobre Crimes Cibernéticos, o primeiro tratado internacional sobre crimes cometidos através da internet e de outras redes de computadores, surge como um importante ponto de referência. A Convenção, adotada pelo Conselho da Europa em 2001 e atualmente ratificada por muitos países ao redor do mundo, oferece uma resposta internacional coordenada ao desafio da cibercriminalidade.

Dessa forma, a adesão à Convenção oferece vários benefícios para o Brasil, incluindo um marco legal amplamente reconhecido e aceito para crimes cibernéticos, acesso à cooperação internacional na investigação e processamento desses crimes, e orientação na elaboração e adaptação da legislação nacional para lidar de forma eficaz e atualizada com a cibercriminalidade.

Nesse contexto, em dezembro de 2019, o Brasil foi convidado a aderir à Convenção, e em julho de 2021, o presidente Jair Bolsonaro encaminhou o processo de ratificação legislativa ao Congresso Nacional. Após aprovação tanto da Câmara dos Deputados quanto do Senado, o Brasil promulgou oficialmente a Convenção sobre o Crime Cibernético por meio do Decreto nº 11.491, publicado no

---

[61] BRASIL. **Decreto-Lei nº 2.848**, de 7 de dezembro de 1940. Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso: 01 jun. 2023

[62] MINISTÉRIO PÚBLICO FEDERAL. **Convenção de Budapeste.** 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacaotematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-dobrasil/docs_legislacao/convencao_cibercrime.pdf. Acesso: 01 jun. 2023

Diário Oficial da União em 12 de abril de 2023[63]. Esta ação fortalece a cooperação do Brasil com parceiros estratégicos na luta contra os crimes cibernéticos, sendo um avanço estratégico que pode aumentar a eficácia da resposta brasileira aos desafios da cibercriminalidade. Portanto, mesmo que esta adesão não resolva todos os desafios que o Brasil enfrenta na luta contra a cibercriminalidade, ela representa um passo significativo em direção a uma abordagem mais robusta, abrangente e atualizada sobre o problema.

Com a adesão, o Brasil tem a oportunidade de melhorar suas capacidades de investigação e processamento de crimes cibernéticos, além de outros crimes que exigem a obtenção de provas eletrônicas/digitais armazenadas em outros países. No entanto, o cenário legislativo brasileiro em relação à cibercriminalidade apresenta-se com desafios relevantes, mesmo que a adesão à Convenção de Budapeste marque um avanço significativo, é imprescindível que o Brasil continue a trabalhar na atualização e fortalecimento de sua própria legislação interna. Com medidas estratégicas, investimentos em capacitação e recursos, além de uma abordagem legislativa robusta e atualizada, o Brasil tem potencial para criar um ambiente legal mais seguro e eficaz no combate à cibercriminalidade.

Na sequência, será estudado os desafios encontrados na rastreabilidade e sanção de condutas criminosas online, diante a crescente sofisticação das técnicas de ocultação de identidade, localização e atividades online, torna-se cada vez mais difícil localizar e punir os responsáveis por atividades criminosas na internet. Dessa forma, se verifica as dificuldades impostas pela natureza descentralizada e global da internet, a qual permite a execução de atividades ilegais a partir de qualquer parte do mundo, além dos problemas associados à coleta e preservação de provas digitais.

4.1. COMPLICAÇÕES NA RASTREABILIDADE E NA SANÇÃO DE CONDUTAS CRIMINOSAS ONLINE

Ao analisar a trajetória da humanidade, percebe-se claramente que o progresso e a busca incessante por inovação são elementos inerentes à natureza humana. Entretanto, mostra-se crucial reconhecer que até mesmo o progresso tem

---

[63] SEGURANÇA,Justiça. **A Convenção de Budapeste é promulgada no Brasil**. Disponível em https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso: 27.mai.2023

seu lado sombrio, no qual indivíduos mal intencionados exploram a inovação e o desconhecimento alheio para realizar ações prejudiciais, e muitas vezes criminosas, e é neste cenário que os crimes virtuais encontram seu nascedouro.

A internet, sem dúvida, figura como a ferramenta mais revolucionária e benéfica já desenvolvida, em razão de sua versatilidade e inúmeros benefícios que proporciona. Com a contínua evolução da sociedade e a expansão constante do acesso à internet, surgem novas demandas.[64] Desta forma, a constante inovação tecnológica gerou novas formas de ameaças, viabilizando a execução de crimes já conhecidos por novos meios, bem como a emergência de delitos antes inimagináveis. Nesse contexto, o Direito enfrenta o desafio de se adaptar para cumprir seu principal objetivo, proteger os bens juridicamente tutelados.

Frente a isso, a evolução da internet e suas correspondentes formas de comunicação, sem uma proteção adequada, proporcionaram um novo cenário para a criminalidade. Nesse cenário, os criminosos exploram as vulnerabilidades dos sistemas e usuários da rede para cometer uma ampla gama de delitos. A rápida emergência de novas formas de criminalidade, a dinâmica da tecnologia da informação, combinada ao anonimato predominante na rede, representam um desafio significativo para os profissionais do Direito no processo de investigação, punição e repressão dos crimes cibernéticos.[65] Logo, as normas jurídicas que guiam a ação do Estado se tornam defasadas diante da evolução e ramificação crescente dos delitos digitais.

Nesse contexto, embora o número de vítimas desses crimes virtuais esteja em crescimento, a quantidade de indivíduos devidamente punidos por cometer tais crimes permanece notavelmente baixa. Isso ressalta a necessidade urgente de desenvolver estratégias mais eficazes e ferramentas legais mais robustas para combater a ameaça dos crimes cibernéticos. Todavia, atualmente o panorama do crime cibernético é multifacetado e está em constante expansão.

---

[64]CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. **Revista científica eletrônica do curso de direito.** 13ª Ed. Disponível em http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso: 01 jun. 2023

[65] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos:** dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. Disponível em https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade. Acesso 05. mai. 2023

Sob esse viés, afirma-se que o principal fator que dificulta a investigação e repressão dos crimes cometidos na rede é a própria natureza da internet. Em que não existem fronteiras e controle centralizado, a internet, com a volatilidade de seus dados e a possibilidade de utilização de ferramentas que dificultam o rastreamento das condutas criminosas, torna a investigação ainda mais desafiadora.

Em 2014, um relatório conjunto da Organização dos Estados Americanos (OEA) e da Symantec, empresa líder em segurança cibernética, trouxe à tona dados preocupantes, indicando que o Brasil figura entre os países da América Latina que mais geram atividades mal-intencionadas na internet.[66] De forma alarmante, o país apresenta o menor índice de denúncias e correspondentes punições para tais atos. Frequentemente, as vítimas não reportam esses incidentes às autoridades competentes, em grande parte devido à desconfiança em relação à eficácia da resposta estatal.

Conforme apontado por Tadeu Rover na revista Consultor Jurídico (CONJUR), a situação do cibercrime no Brasil é preocupante. No ano de 2016, mais de 42 milhões de cidadãos brasileiros foram vítimas de atividades criminosas online. Esse número representou um incremento de 10% em relação ao ano anterior, segundo dados da Norton, uma companhia renomada no campo de soluções de segurança cibernética.[67]

As complexidades e desafios associados à investigação, identificação e repressão desses crimes pelos órgãos estatais aumentam a dificuldade em conter tais delitos. Como resultado, a criminologia crítica denomina esse fenômeno como a "cifra negra" da criminalidade, um termo que se refere à subnotificação de crimes às autoridades estatais. Portanto, é imperativo planejar medidas para encorajar as vítimas a denunciar os cibercrimes e melhorar a capacidade das autoridades em investigar e punir esses delitos.

Existem inúmeras complicações e desafios no processo penal voltado ao combate e punição de cibercrimes. A polícia, o Ministério Público, o poder judiciário, legisladores e outros profissionais jurídicos enfrentam obstáculos significativos que

---

[66] SYMANTEC. BROADCOM INC. Organizações dos Estados Americanos. Relatório '**Tendências de Cibersegurança na América Latina e no Caribe**". 2014. Disponível em https://www.broadcom.com/404-symantec?sourceURL=http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc-annex.pdf. Acesso 05. mai. 2023

[67] ROVER, Tadeu. **Violência virtual: i**nternet facilita crimes e dificulta investigação, estimulando a impunidade. Disponível em https://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais. Acesso 05. mai. 2023

dificultam a execução do direito de punir e incentivam a atividade criminosa, mesmo que a legislação brasileira tenha penas para crimes cibernéticos e leis que protegem a privacidade e os dados dos usuários. No entanto, ainda são necessários a criação de mecanismos que facilitem a investigação e repressão dos crimes digitais, mesmo que a natureza volátil e transitória dos dados digitais torne a investigação de crimes cibernéticos um desafio.[68]

A tecnologia da informação, marcada por seu caráter dinâmico e volátil, propicia uma variedade quase ilimitada de métodos para a execução de crimes cibernéticos. Com isso, quando iniciado o processo penal, por meio da investigação de um crime virtual cometido, é crucial identificar rapidamente o meio pelo qual o crime foi praticado. Essa identificação é fundamental para orientar as ações da entidade investigativa, pois as técnicas utilizadas para determinar a autoria e a materialidade do crime variam conforme o meio utilizado pelo cibercriminoso para realizar o ato ilícito. Ao ponto que os desafios começam com o fato de que, no sistema jurídico brasileiro, há uma necessidade predominante de demonstrar com evidências robustas a autoria e a materialidade do delito para que a sanção penal possa ser aplicada. Esta necessidade de comprovação forte e inequívoca de autoria é um dos principais obstáculos no processo penal relativo aos cibercrimes.

Caso não consiga ser comprovada a materialidade e autoria o juiz deverá absolver o réu, conforme traz o artigo 386 do Decreto-lei nº 3.689, de 3 de outubro de 1941(Código de Processo Penal):

> Art. 386. O juiz absolverá o réu, mencionando a causa na parte dispositiva, desde que reconheça:
> I - Estar provada a inexistência do fato;
> II - Não haver prova da existência do fato;
> III - Não constituir o fato infração penal;
> IV - Estar provado que o réu não concorreu para a infração penal;
> V - Não existir prova de ter o réu concorrido para a infração penal;
> VI – existirem circunstâncias que excluam o crime ou isentem o réu de pena, ou mesmo se houver fundada dúvida sobre sua existência;
> VII – não existir prova suficiente para a condenação.

Nesse contexto, o primeiro e mais complexo obstáculo na investigação destes crimes é estabelecer a autoria do crime, o que é particularmente desafiador

---

[68] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos:** dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. Disponível em https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade. Acesso 05. mai. 2023

devido à natureza anônima e difusa da internet. A obtenção e coleta dessas provas são um processo intrincado e precisa estar em estrita conformidade com a lei, em respeito ao princípio da legalidade, para evitar violações e nulidades. Dessa forma, a natureza anônima do indivíduo na internet, muitas vezes, leva a uma sobreposição de direitos fundamentais, como o direito a privacidade, confidencialidade de dados, e a necessidade de proteção contra atividades criminosas.

Devido a própria estrutura da rede de internet, que permite o anonimato por meio do uso de endereços IP dinâmicos, *proxies* e técnicas de roteamento. Mesmo que, os registros de IP e os *logs* são peças cruciais de evidências nas investigações de crimes digitais, a obtenção dessas provas não é uma tarefa simples, há uma série de exigências legais que devem ser cumpridas para garantir a legalidade do processo e evitar a contaminação da prova.[69]

Sendo assim, os desafios de investigar e reprimir os crimes são vastos e complexos, conforme discutido na primeira audiência pública da Comissão Parlamentar de Inquérito dos Crimes Cibernéticos realizada em 2014. Na época, o Delegado Elmer Coelho Vicente, Chefe do Serviço de Repressão aos Crimes Cibernéticos da Polícia Federal, evidenciou a disparidade entre a velocidade de realização desses crimes e o ritmo para obtenção dos dados necessários para as investigações.[70] Entre as principais dificuldades enfrentadas pelas autoridades policiais, destacam-se após o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014)[71], diante a resistência de empresas em fornecer informações sem ordem judicial e a complexidade inerente ao rastreamento de atividades cibernéticas, devido ao uso de *proxies* e da técnica de roteamento, que permite aos usuários ocultar sua localização e identidade na web. Logo, os sites e provedores de acesso à internet são os principais repositórios de informações sobre a utilização da plataforma, onde tais registros são armazenados.

---

[69] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos:** dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. Disponível em https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios da-autoria-e-prova-da-materialidade. Acesso: 15 abr. 2023

[70] CANUTO, Luiz Cláudio. **CPI constata dificuldade em rastrear e punir crimes de internet.** Disponível em https://www.camara.leg.br/noticias/467819-cpi-constata-dificuldade-em-rastrear-e-punir-crimes-deinternet/. Acesso: 15 abr. 2023

[71] BRASIL. Marco civil da internet: Lei n. 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 2. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2015.

No entanto, a maior parte desses dados não é mantida por um período extenso. Desta maneira, fica notório que a demora na obtenção dessas informações e, por consequência, no avanço das investigações, pode causar danos irreparáveis, como a perda total dessas informações. Ademais, além da perda de dados por descarte após um certo tempo por parte dos próprios provedores, as evidências de crimes digitais podem ser facilmente apagadas ou alteradas pelos usuários. Isso pode levar a destruição, ou ao menos, a modificação das provas do crime. Consequentemente, a necessária reserva jurisdicional, a lentidão de todo o procedimento para acessar corretamente os dados e provas do crime, resultam em uma investigação extremamente morosa. Esta lentidão, não raro, pode culminar na prescrição do delito, sem que haja progressos significativos na fase inquisitorial.

Em contrapartida, uma vez que todos os trâmites legais foram seguidos e a identificação do criminoso através dos dados e informações fornecidos pelos sites e provedores de acesso tornou-se possível, a investigação passará a se dedicar à busca de provas da materialidade do crime virtual cometido pelo agente. Dessa forma, mostra-se fundamental a realização de perícia técnica para produção de prova hábil a lastrear uma criminalização do agente.

Sob essa perspectiva, mesmo que exista legislação tipificando tais crimes, incluindo o Código Penal, o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), há uma demanda complexa no combate aos cibercrimes desde a identificação até a efetiva punição, o qual requer uma abordagem abrangente e colaborativa em todos os níveis da sociedade.

O Ministério da Justiça e Segurança Pública (MJSP), representando o Governo Federal, inaugurou o pioneiro Plano Tático de Combate a Crimes Cibernéticos. Assim, o projeto tem como propósito mitigar e prevenir a incidência de delitos digitais no Brasil. Um marco deste Plano Tático é um Acordo de Cooperação estabelecido entre a Polícia Federal e a Federação Brasileira de Bancos (Febraban)[72]. Este acordo permitirá uma troca mais eficaz de informações com o intuito de promover medidas educativas e preventivas para garantir uma esfera cibernética mais segura, além de identificar e punir grupos criminosos. A Febraban, uma instituição privada, desempenhou um papel significativo na criação e incentivo

[72]MINISTÉRIO DÁ JUSTIÇA E SEGURANÇA PÚBLICA. **Plano Tático de Combate a Crimes Cibernéticos.** Disponível em https://www.gov.br/mj/pt-br/assuntos/noticias/ministerio-da-justica-e-seguranca-publica-lanca-plano-tatico-de-combate-a-crimes-ciberneticos. Acesso 07. mai. 2023

do Plano Tático de Combate, alegando ter evitado danos financeiros de aproximadamente R$ 4 bilhões aos seus clientes somente no ano de 2021[73].

O Plano Tático contempla a implantação de um repositório de dados sobre ocorrências cibernéticas, acessível às polícias judiciárias, federais e estaduais, no qual permitirá que as estratégias e soluções de investigação de crimes sejam efetivamente replicadas em todo o país. Ademais, o plano propõe a criação de um programa dedicado a prevenção de fraudes bancárias onlines e golpes digitais, além de prover treinamento especializado para os agentes de segurança. Outro ponto importante é a estruturação de um sistema integrado, que contará com a colaboração de forças de segurança federais e estaduais, entidades nacionais e internacionais, tanto públicas quanto privadas, bem como de especialistas em segurança digital.

Dessa forma, o Plano Tático é organizado em torno de eixos temáticos, que abordam a prevenção e redução de ameaças cibernéticas, desde o gerenciamento de riscos e incidentes ligados à criminalidade cibernética, ao aprimoramento de infraestruturas críticas para o combate desses crimes. Este projeto está alinhado com as diretrizes estabelecidas pelo Decreto n.º 10.222/2020, que ratificou a Estratégia Nacional de Segurança Cibernética (E-Ciber)[74].

No entanto, a atual legislação brasileira ainda enfrenta dificuldades em combater efetivamente esses crimes cibernéticos. Os desafios desses delitos, como sua complexidade, o problema na coleta de evidências e a escassez de equipes qualificadas, criam empecilhos no caminho para a justiça. Nesse cenário, é de suma importância investir na capacitação de profissionais e aprimorar a cooperação internacional no âmbito das investigações de cibercrimes.

Um passo vital na prevenção desses crimes é a sensibilização dos usuários quanto à segurança online e à proteção de seus dados pessoais. Além disso, é indispensável fomentar a pesquisa, o desenvolvimento e a educação na área de segurança cibernética como estratégias para combater esses crimes.

---

[73] MINISTÉRIO DÁ JUSTIÇA E SEGURANÇA PÚBLICA. **Plano Tático de Combate a Crimes Cibernéticos.** Disponível em https://www.gov.br/mj/pt-br/assuntos/noticias/ministerio-da-justica-e-seguranca-publica-lanca-plano-tatico-de-combate-a-crimes-ciberneticos. Acesso:15 abr. 2023

[74] SEGURANÇA PÚBLICA, **Governo Federal lança Plano Tático de Combate a Crimes Cibernéticos.** 2022. Disponível em https://www.gov.br/pt-br/noticias/justica-e-seguranca/2022/03/governo-federal-lanca-plano-tatico-de-combate-a-crimes-ciberneticos. Acesso: 18. mai.2023

Na sequência, será abordada uma questão crítica que amplia a complexidade da luta contra a cibercriminalidade: os impasses do anonimato nas redes. O anonimato, como veremos, é um duplo gume na esfera digital. Por um lado, é uma ferramenta importante para garantir a liberdade de expressão, a privacidade e a segurança dos usuários. Por outro lado, cria um ambiente propício para o cometimento de crimes, uma vez que oferece um escudo contra a identificação e, consequentemente, a responsabilização.

4.2. OS IMPASSES DO ANONIMATO NA INTERNET E SEUS REFLEXOS NA CIBERCRIMINALIDADE

O anonimato pode se tornar um obstáculo significativo na investigação e punição de crimes cibernéticos, uma vez que torna a identificação e a localização dos autores muito mais desafiadoras. Este capítulo irá explorar a fundo essa problemática, descrevendo os dilemas e desafios relacionados ao anonimato nas redes e como isso impacta a segurança cibernética, a investigação de crimes e a aplicação da lei. Além disso, se evidenciará as possíveis soluções para este impasse e como a legislação nacional e internacional vem tentando lidar com essa questão.

Nesse viés, o direito a privacidade se mostra fundamento no universo digital, constituindo-se como o direito mais valorizado para o bom funcionamento das ferramentas e recursos disponíveis neste ambiente. Paralelamente, nota-se um crescimento vertiginoso nas taxas de crimes cibernéticos, bem como o surgimento contínuo de novos mecanismos que facilitam a ocorrência desses delitos. Essas práticas prejudiciais a direitos de terceiros, que frequentemente se qualificam como criminosas, demandam ações de combate robustas para responsabilizar e punir seus autores, reprimindo a impunidade, assegurando o exercício integral dos direitos individuais e coletivos, protegendo os cidadãos e, por consequência, preservando o Estado Democrático de Direito.[75] Logo, no âmbito digital, onde as relações interpessoais e as atividades diárias encontram-se cada vez mais imersas,

---

[75]MORAES, Paulo Francisco Cardoso de. A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores. **Revista Âmbito Jurídico.** Disponível em https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/ Acesso: 2.jun.2023.

o anonimato ganhou novos contornos e desafios, sendo um assunto de relevância jurídica e social, pois abrange diversas questões complexas que envolvem privacidade, liberdade de expressão, segurança da informação e responsabilidade legal.

No nascimento da internet, a garantia do anonimato dos usuários era um de seus principais objetivos. Esse recurso visava assegurar que os usuários, ao permanecerem não identificáveis, pudessem utilizar de forma mais eficiente os recursos oferecidos, promovendo a igualdade entre todos no ambiente virtual.[76] Contudo, a internet, tal como foi concebida originalmente, buscando que seus usuários permaneçam não identificados, confronta-se, em várias situações, com o que a Constituição prescreve. Assim com o aparecimento e crescimento expressivo dos delitos cometidos na internet e contra suas ferramentas de uso, a prerrogativa do anonimato teve que ser reavaliada e equilibrada no contexto social onde estava inserida, levando em conta à Constituição Federal de 1988 e as leis infraconstitucionais subsequentes. Ainda que a Constituição proíba o anonimato, este continua sendo uma das principais origens dos crimes virtuais, pois facilita a impunidade dos delitos perpetrados na rede.

Ao ponto que é um direito fundamental garantir o respeito a privacidade, a intimidade, ao sigilo e a livre manifestação do pensamento nas redes informáticas, uma vez que são garantias constitucionais, isso deve ser realizado de maneira equilibrada, buscando a proteção dos direitos de terceiros de maneira que não se viole os direitos fundamentais e os direitos humanos.

Sob essa perspectiva, o maior desafio neste contexto envolve sistemas que operam com redes anônimas, conhecidas como *Deep Web* e *Dark Web*. Devido ao fato de que suas páginas não são localizadas pelos motores de busca convencionais e de que seus programas possuem criptografias sofisticadas, o que torna, na maioria das vezes, impossível a identificação de seus usuários. Esses fatores, e a sensação de garantia de impunidade que eles proporcionam, facilitam que os mais variados tipos de crimes sejam executados neste ambiente.

---

[76] 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://sistemas.uft.edu.br/periodicos/index.php/direito/article/view/23590106.2017v4n2p191#:~:text=O%20presente%20artigo%20busca%20compreender,Leis%20Penais%20regulando%20esse%20crime. Acesso em 16 abr. 2023

A nossa sociedade, consagra o pluralismo de ideias e pensamentos, bem como o respeito e a tolerância, como necessidades vitais para a convivência entre as pessoas. Neste contexto, a liberdade de expressão é fundamental e abrange não apenas informações consideradas inofensivas, indiferentes ou favoráveis, mas também aquelas que podem provocar perturbações, resistência ou inquietar pessoas.[77]

Reafirmando a importância do direito à liberdade de expressão, a Declaração Universal dos Direitos do Homem, no qual o Brasil é signatário, em seu artigo 19, estabelece que "todo homem tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferências, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras".[78]

Nessa linha, a Constituição Federal Brasileira de 1988 assegura, em seu art. 5º, IV, que “é livre a manifestação do pensamento, sendo vedado o anonimato”[79]. Este documento fundamental ainda protege essa liberdade em várias outras passagens, dada a sua importância.

Neste sentido, é preciso lembrar alguns artigos que, direta ou indiretamente, asseguram essa liberdade primordial aos cidadãos, tais como: o art. 5º, X, que protege a intimidade, a vida privada, a honra e a imagem das pessoas; o XIV, que garante o acesso à informação e resguarda o sigilo da fonte, quando necessário ao exercício profissional; e o art. 220, que protege o direito à manifestação do pensamento, à criação, à expressão e à informação, sob qualquer forma, processo ou veículo, de acordo com a Constituição.[80]

Como sublinha Alexandre de Moraes[81]:

> O Estado democrático defende o conteúdo essencial da manifestação da liberdade, que é assegurada tanto no aspecto positivo, isto é, na proteção da expressão de opinião, quanto no aspecto negativo, referente à proibição da censura.

---

[77] MORAES, Alexandre de. **Constituição do Brasil interpretada e legislação constitucional.** 4. ed. – São Paulo: Atlas, 2004. p 207.

[78] **Declaração Universal dos Direitos do Homem.** Disponível em http://pfdc.pgr.mpf.mp.br/atuacao-econteudos-de-apoio/legislacao/direitos-humanos/declar_dir_homem.pdf. Acesso 08. mai. 2023

[79] BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal: Centro Gráfico, 1988.

[80] BRANCO, Paulo Gustavo Gonet; COELHO, Inocêncio Mártires; MENDES, Gilmar Ferreira. **Curso de Direito Constitucional**. 4ª. ed. São Paulo: Saraiva, 2008. p. 404.

[81] MORAES, Alexandre de. **Direito constitucional.** 15. Ed. – São Paulo: Atlas, 2004. p. 74

A liberdade de expressão, entendida como um direito fundamental inerente à pessoa humana, visa inibir a censura estatal. No entanto, essa liberdade será limitada sempre que necessário, em casos de conflito entre ela e outros direitos fundamentais ou valores constitucionais distintos. A proibição constitucional à censura não impede que o indivíduo seja responsabilizado civil, penal ou administrativamente pelas consequências de seus atos.

Fica evidente que ninguém pode invocar seu direito à liberdade de expressão como forma de contrapor-se à proibição constitucional do anonimato.

Nesse sentido, se mostra necessário observar também a Lei Geral de Proteção de Dados (LGPD), que estabelece diretrizes rigorosas sobre como as empresas e organizações devem tratar os dados pessoais dos usuários, incluindo a obrigação de garantir a segurança desses dados e o direito do titular à anonimização de seus dados, quando possível. Globalmente, os problemas associados ao anonimato na internet são igualmente desafiadores. A dificuldade de rastrear e identificar usuários anônimos pode resultar em uma série de abusos, como a disseminação de discursos de ódio, a propagação de notícias falsas, a prática de crimes virtuais e até a evasão de responsabilidades legais. Por outro lado, o anonimato pode ser crucial para proteger indivíduos em situações vulneráveis ou que precisem denunciar crimes ou irregularidades sem o medo de represálias. No mais, a questão do anonimato nas redes sociais possui uma forte ligação com a noção contemporânea de privacidade. A medida, que cada vez mais aspectos de nossas vidas se tornam digitalmente públicos, o direito à privacidade tornou-se um tópico de grande importância.

Diante deste panorama, o anonimato vivifica-se como uma faceta complexa. Em um aspecto positivo, pode ser um instrumento de proteção da liberdade de expressão e privacidade do indivíduo, permitindo, por exemplo, que dissidentes políticos ou grupos vulneráveis expressem suas opiniões sem receio de represálias. Por outro lado, o anonimato também pode ser utilizado como uma ferramenta que auxilia na perpetração de atividades ilícitas na rede, incluindo os crimes cibernéticos, e na evasão da aplicação da lei. Os desafios trazidos pelo anonimato são muitos e multifacetados. A segurança cibernética é diretamente afetada, uma vez que pessoas mal intencionadas podem esconder suas identidades enquanto lançam ataques virtuais, tornando a prevenção, detecção e resposta a esses

ataques extremamente desafiadoras. Da mesma forma, que a investigação de tais crimes é prejudicada pela capacidade dos criminosos de permanecerem desconhecidos, dificultando a coleta de provas e a imputação de responsabilidades.

Sendo assim, a aplicação da lei também enfrenta empecilhos significativos posto que as autoridades judiciais e policiais muitas vezes se veem impossibilitadas de rastrear e identificar os perpetradores de crimes cibernéticos, o que leva a uma taxa de impunidade preocupante que dificulta a dissuasão de tais crimes. Como resposta a essa problemática, várias soluções têm sido propostas e implementadas, tanto em âmbito nacional como internacional. Entre elas, destaca-se a implementação de legislações mais rigorosas e específicas para crimes cibernéticos, a criação de equipes especializadas de investigação e a cooperação internacional para aperfeiçoar o rastreamento e a identificação de criminosos cibernéticos.

Por outro lado, essas medidas também levantaram questões sobre a proteção dos direitos individuais e da privacidade. Portanto, encontrar um equilíbrio adequado entre a necessidade de proteção contra crimes cibernéticos e a preservação do anonimato e privacidade dos usuários constitui um desafio crucial.

Em âmbito internacional, a Convenção de Budapeste se mostra como um exemplo de esforço para lidar com a questão do anonimato na rede e seus impactos na cibercriminalidade. Contudo, a efetividade desta e de outras convenções internacionais ainda é um ponto de debate e depende muito da adesão e implementação adequada pelos países membros. Assim, o presente capítulo buscou aprofundar a discussão desses dilemas e desafios.

4.3. CONVENÇÃO DE BUDAPESTE

A ascensão do uso de ferramentas online revolucionou nossas atividades cotidianas, trazendo a comodidade do mundo virtual ao alcance de nossas mãos. Contudo, seu uso inadequado apresentou sérios riscos para a segurança de indivíduos e nações, colocando seus bens e direitos em perigo. Por isso, a Convenção sobre o Cibercrime foi estabelecida com o propósito de enfrentar essas ameaças digitais em um contexto global[82], desempenhando um papel importante na

[82]CONVENÇÃO de Budapeste. 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacaotematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-dobrasil/docs_legislacao/convencao_cibercrime.pdf. Acesso 05. mai. 2023

definição de normas internacionais para a investigação e a repressão de delitos cibernéticos.

Deste modo, o processo que levou a criação da Convenção de Budapeste teve início no final dos anos 1990, quando o crescimento exponencial da internet e da tecnologia digital despertou preocupações sobre a sua possível exploração para fins criminosos. Em resposta a esse desafio emergente, o Conselho da Europa - uma organização internacional dedicada à promoção da democracia, dos direitos humanos e do Estado de Direito na Europa - iniciou um processo de consulta para desenvolver um instrumento jurídico internacional para o cibercrime. Após várias rodadas de consultas e negociações que envolveram não apenas os Estados membros do Conselho da Europa, mas também países não membros, como os Estados Unidos, o Canadá, o Japão e a África do Sul, o projeto da Convenção foi concluído em 2001, no rescaldo do trágico evento terrorista de 11 de setembro de 2001 nos Estados Unidos, a Comunidade Europeia promoveu a Convenção sobre o Cibercrime em Budapeste, capital da Hungria. A meta era padronizar a repressão aos crimes virtuais globalmente, levando em conta sua principal característica, a transnacionalidade.[83]

Por conseguinte, em 23 de novembro de 2001, Budapeste se tornou o palco de debates e assinaturas que culminaram na criação da Convenção de Budapeste sobre o Cibercrime, a maior convenção internacional sobre crimes cibernéticos. Entrou em vigor no âmbito jurídico internacional em 1º de julho de 2004, após as cinco ratificações necessárias, introduziu o termo "cibercrime" no sistema jurídico internacional, além de tipificar os principais delitos cometidos no espaço virtual.[84] Bem como, estabeleceu normas de direito penal e processual penal com a intenção de definir ações conjuntas entre os países signatários para a tipificação, investigação e combate aos crimes cometidos através e contra a internet.

Dessa forma, o objetivo central da Convenção consistem em fomentar e facilitar a cooperação internacional no combate aos crimes cibernéticos, dando prioridade a uma política criminal comum para proteger a sociedade contra a criminalidade no ciberespaço, notavelmente por meio da adoção de legislação

---

[83] VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos:** a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso. **Revista da ESMAPE.** Recife. v. 15. n. 32. p. 239.

[84] ROMANO, Rogério Tadeu. CONVENÇÃO DE BUDAPESTE E CIBERCRIMES. Disponível em. https://jus.com.br/artigos/72969/convencao-de-budapeste-e-cibercrimes. Acesso: 5. jun. 2023.

adequada e melhor cooperação internacional, investigações e processos relacionados a delitos cibernéticos e promover a integridade dos sistemas de informação.[85]. Com isso, a cooperação estipulada na convenção, inclui normas processuais para a coleta de provas e normas de direito substantivo para a criação de delitos puníveis cometidos no espaço virtual.

Embora a Convenção de Budapeste tenha sido criticada por alguns países e organizações devido a preocupações sobre a privacidade e a liberdade de expressão, ela se tornou um referencial importante na luta contra o cibercrime em nível global. Assim, este marco representa o primeiro instrumento jurídico transnacional para a regulamentação da internet, fornecendo um modelo e parâmetro a ser adotado nas legislações dos países signatários e influenciando a doutrina e as decisões judiciais dos países não signatários, dada a sua importância no tema.

> Segundo seu Preâmbulo, a Convenção prioriza uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional e reconhece a necessidade de uma cooperação entre os Estados e a indústria privada[86].

A Convenção enfatiza, desde sua concepção, o respeito à Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa (1950), ao Pacto Internacional sobre os Direitos Civis e Políticos da ONU (1966), à Convenção das Nações Unidas sobre os Direitos da Criança (1989), e à Convenção da Organização Internacional do Trabalho sobre as Piores Formas do Trabalho Infantil (1999)[87].

Sob essa ótica, a Convenção, sob sua perspectiva jurídica, define e categoriza cibercrimes em diversas infrações: aquelas contra sistemas e dados informáticos, delitos associados ao uso de computadores, infrações de conteúdo

---

[85] Secretaria Geral da Presidência da República. **Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética**. Disponível em https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica. Acesso: 9.maio.2023

[86] **MINISTÉRIO PÚBLICO.** Convenção de Budapeste. 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacaotematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-dobrasil/docs_legislacao/convencao_cibercrime.pdf. Acesso 05. mai. 2023

[87] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A Convenção de Budapeste e as Leis Brasileiras.** Disponível em. https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras. Acesso 08. mai. 2023

específico como pornografia infantil, e violações relacionadas a direitos autorais. Sua elaboração visou não apenas a introdução de novas categorias criminais, mas também a definição de diretrizes para procedimentos penais, integrando práticas de direito penal internacional e estabelecendo normas relativas à tecnologia da informação. Adicionalmente, a convenção incentiva os países signatários a implementar legislações internas que classifiquem e criminalizem outros tipos de crimes cibernéticos. O foco também recai sobre aspectos processuais, buscando garantir que as autoridades relevantes tenham regulamentos bem definidos para cooperar na persecução penal de crimes digitais. Nesse sentido, objetiva-se implementar mecanismos de cooperação internacional ágeis e eficazes para enfrentar tais delitos.

Dessa forma, lida com temas cruciais relacionados à coleta de provas, como identificação, armazenamento e conservação de dados informáticos, busca e apreensão de dados virtuais, entre outros procedimentos. Logo, em termos de cooperação internacional, a Convenção se mostra flexível, permitindo as partes envolvidas escolherem a jurisdição mais adequada para o caso em questão. Em relação a extradição, a Convenção prevê que esta medida está sujeita às condições estabelecidas pela legislação do país requerido ou pelos tratados de extradição aplicáveis.

Atualmente, a Convenção possui mais de 60 Estados-partes signatários e conta com outros 10 países observadores.[88] O Brasil, embora não tenha aderido à Convenção de Budapeste no momento de sua criação, iniciou conversas com o Conselho da Europa em julho de 2019 e expressou sua intenção de aderir à Convenção. Por conseguinte, em dezembro de 2019, o Comitê de Ministros do Conselho da Europa convidou o Brasil para aderir à Convenção.

> Trata-se de iniciativa decorrente de trabalho de coordenação interinstitucional, constituído para esse fim, entre o Ministério das Relações Exteriores, a Polícia Federal (PF) e o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) – ambos do Ministério da Justiça e Segurança Pública –, o Gabinete de Segurança Institucional da Presidência da República, a Agência Brasileira de Inteligência e o Ministério

[88] KAMINSKI, Omar. Conheça o Tratado Internacional contra crimes na Internet. **Revista Consultor Jurídico.** Disponível em . https://www.conjur.com.br/2001-nov-4/convencao_lanca_tratado_internacional_cibercrimes. Acesso: 2.jun.2023

> Público Federal. O Ministro da Justiça e Segurança Pública, Sergio Moro, fez o pedido com base em pareceres técnicos da PF e do DRCI. [89]

A adesão a Convenção, proporciona as autoridades brasileiras um acesso mais amplo e ágil às provas eletrônicas e outros elementos informativos sob jurisdição estrangeira, além de tornar mais efetiva a cooperação jurídica internacional no combate a esses crimes.

Desta forma, em julho de 2020, o texto da Convenção sobre Cibercrime foi encaminhado ao Congresso Nacional para análise e possível ratificação da participação brasileira. Contudo, mesmo durante o período de conclusão dos procedimentos legais para a assinatura da Convenção Internacional, o Brasil já tinha a possibilidade de participar das reuniões e respectivos protocolos na posição de observador.

A iniciativa de adesão do Brasil à Convenção de Budapeste sobre a criminalidade virtual está alinhada com os objetivos da Lei n.º 12.965/2014, conhecida como Marco Civil da Internet, visando proporcionar meios adequados para a persecução penal dos crimes cibernéticos. Com a internet inserindo características peculiares aos crimes virtuais, é imperativo que a abordagem para combater essas infrações seja rápida, impedindo atos criminosos em curso e elucidando com sucesso delitos já cometidos.

Apesar da existência de leis nacionais que se preocupam com pontos importantes para a persecução penal de crimes virtuais, a criminalidade digital não conhece fronteiras. Nesse cenário, a adesão do Brasil à Convenção de Budapeste se mostrou necessária para complementar nossa legislação nacional, que ainda apresenta deficiências na área, estabelecendo diretrizes mais tangíveis para a persecução penal de crimes virtuais[90].

Portanto, o Brasil ao se tornar signatário do referido acordo de cooperação internacional, se insere em um regime internacional de combate ao cibercrime, facilitando a comunicação e colaboração com outros países que enfrentam práticas ilícitas semelhantes, mas com legislações e regras de persecução penal distintas.

---

[89] Ministério das Relações Exteriores. **Processo de adesão à Convenção de Budapeste** -Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública. Disponível em http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-

[90] Brasil adere à Convenção de Budapeste e se posiciona contra crimes cibernéticos. Disponível em https://diariodoturismo.com.br/brasil-adere-a-convencao-de-budapeste-e-se-posiciona-contra-crimes/ .

No entanto, embora a adesão à Convenção seja um passo significativo para o aprimoramento do combate aos crimes cibernéticos, ela deve ser complementada por esforços domésticos contínuos para manter a legislação atualizada. Na próxima parte deste estudo, se evidencia a discussão sobre a incorporação da Convenção de Budapeste ao ordenamento jurídico brasileiro, tendo em vista a etapa crucial na jornada do Brasil para fortalecer sua estrutura legal e estratégica no enfrentamento dos cibercrimes. Bem como os desafios, as oportunidades e as implicações desta importante adesão, bem como as mudanças necessárias na legislação interna e os possíveis impactos sobre as práticas de investigação e jurisprudência existentes. Ademais, vamos explorar como essa incorporação pode afetar a interação do Brasil com outros países na área digital e no âmbito da cooperação internacional para a segurança cibernética.

4.4. A INCORPORAÇÃO DA CONVENÇÃO DE BUDAPESTE NO ORDENAMENTO JURÍDICO BRASILEIRO

A participação da República Federativa do Brasil na Convenção sobre o Crime Cibernético, celebrada em Budapeste em 23 de novembro de 2001[91], representou o início de um marco significativo para o país. Este compromisso foi posteriormente ratificado pelo Congresso Nacional, através do Decreto Legislativo n.º 37, formalizado em 16 de dezembro de 2021. Assim, completando o processo de adesão[92], o Governo brasileiro apresentou o instrumento de ratificação da Convenção ao Secretário-Geral do Conselho da Europa em 30 de novembro de 2022, culminando com a entrada em vigor, no plano jurídico internacional, da referida Convenção para o Brasil em 1º de março de 2023. Por conseguinte, foi devidamente incorporada ao sistema jurídico brasileiro, por meio do Decreto 11.491, promulgado em 12 de abril de 2023. Esta sucessão de eventos marca uma nova fase na luta contra o crime cibernético no Brasil, refletindo o compromisso do país com a cooperação internacional e o fortalecimento da segurança cibernética.

---

[91]MINISTÉRIO PÚBLICO. **Convenção de Budapeste.** 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacaotematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-dobrasil/docs_legislacao/convencao_cibercrime.pdf. Acesso 05. mai. 2023

[92] Ministério das Relações Exteriores. Processo de adesão à Convenção de Budapeste -Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública. Disponível em http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de- Acesso 05. mai. 2023

Neste viés, após uma pandemia global, o Brasil passa por um período de recuperação, enfrentando um aumento significativo na ocorrência de crimes cibernéticos, nos quais grandes corporações e até mesmo instituições governamentais foram alvos de ataques de *ransomware*, resultando no sequestro de dados valiosos e subsequentes tentativas de extorsão. Assim, a necessidade de uma estratégia unificada e eficaz para combater o crime organizado no domínio cibernético nunca foi tão evidente.

Os signatários do tratado, desde o início dos anos 2000, já percebiam a crescente tendência do crime organizado em se digitalizar, utilizando a internet como principal meio de operação[93]. Consequentemente, foi imprescindível a construção de uma estratégia comum para combater tal fenômeno, considerando a natureza internacional da rede de internet, que abrange múltiplos sistemas jurídicos. Assim, a Convenção de Budapeste trouxe consigo uma série de benefícios, de modo que ela visa a adoção de legislações adequadas, o estímulo à cooperação internacional entre os Estados e a indústria, o cumprimento das regulações de proteção de dados, bem como das convenções de Direitos Humanos e de Direitos da Criança.

No contexto cibernético, se torna fundamental agir rapidamente, reunindo evidências sólidas, mantendo a integridade dos dados e garantindo a cadeia de custódia para capturar os criminosos. Logo, um dos principais focos da convenção é a coleta e o compartilhamento de dados para investigação. Nesse contexto, os países signatários são obrigados a se ajustar aos conceitos e à gama de crimes estipulados pela Convenção de Budapeste. Ao ponto, que o tratado orienta que os crimes devem ser tratados de maneira uniforme em todas as jurisdições nacionais, garantindo uma reciprocidade na abordagem de crimes que afetam a confidencialidade, integridade e disponibilidade, bem como crimes ligados a conteúdos e violações de direitos autorais, entre outros.

Embora o Brasil tenha demorado para aderir à convenção, tem-se feito esforços para atualizar a legislação penal do país. Avanços notáveis nesse sentido

---

[93] MINISTÉRIO DAS RELAÇÕES EXTERIORES. **Processo de adesão à Convenção de Budapeste** -Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública. Disponível em http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-. Acesso 05. mai. 2023

incluem a aprovação da Lei n.º 14.155, de 27 de maio de 2021[94], no qual alterou o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet, como também o Decreto-Lei n.º 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato.

Portanto, algumas situações previstas na Convenção de Budapeste já estão contempladas em nossa legislação, como o crime de pornografia infantil e crimes relacionados a direitos autorais. No entanto, a Convenção também abrange a proteção jurídica e o combate a uma série de atos que hoje não possuem previsão legal, como, por exemplo, o disposto no artigo 6º, *alínea* a, da Convenção, que identifica como atos criminosos a produção criminosa de informações destinadas à práticas de crimes em ambiente virtual, aparelho ou programa de computador, ou representação, como se explicita no art. 7º. Aparentemente, essas tipificações seriam muito bem recebidas no ordenamento jurídico brasileiro, pois tais condutas se tornaram corriqueiras no âmbito nacional e causam sérios prejuízos aos usuários. Todavia, por não serem tipificadas como ilícitas, acabam passando como condutas brandas e passíveis.[95]

Além disso, um distinto exemplo de ato lesivo praticado em larga escala e causador de graves danos materiais e pessoais e não tipificado na legislação brasileira é o conhecido o golpe de clonagem de *Whatsapp*, em que cibercriminosos cadastram o número do telefone do usuário em outro dispositivo, após este processo, o usuário original tem acesso e recebe um *SMS* contendo um código de liberação de acesso. Com acesso ao código, a vítima é induzida a fornecer esse código ao autor do flagrante, então sua conta no *WhatsApp* é bloqueada, momento em que o autor do crime começa a se passar pela vítima, geralmente pedindo dinheiro a contatos de pessoas que tiveram seu *whatsapp* hackeado, e em alguns casos pode até violar a privacidade pessoal, para acessar fotos, conversas, e outros

---

[94] BRASIL.**Lei 14.155, de 27 de maio de 202**1. Aperfeiçoa a legislação penal e processual penal. Disponível emhttp://https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm Acesso 05. mai. 2023

[95] COLTRO, Rafael Khali. WALDMAN, Ricardo Libel. Criminalidade digital no Brasil: A problemática e a aplicabilidade da convenção de Budapeste. EM TEMPO INSS – 1984 – 7858 DIGITAL.v. 21 n. 01. 2021.

documentos pessoais fornecidos no *software*. Segundo desenvolvido por Coltro,[96] essa prática é tão eficaz que, até fevereiro de 2020, mais de 9 milhões de pessoas já caíram no referido golpe.

No entanto, a falta de tipicidade dificulta o efetivo combate a essas práticas, sendo que a polícia normalmente só investiga quando consegue avaliar o prejuízo financeiro de uma das vítimas e caracteriza a prática como crime de peculato, danos ao caráter ou tentativa de peculato e, em última análise, nem serão investigados. Dito isso, o entendimento geral é que, se não houver prejuízo financeiro para a pessoa que clona o número ou seus contatos no aplicativo, isso não configura crime, pois o peculato requer perda efetiva para constituir configuração criminosa. Logo, os raros casos que passam da fase pré-processual e chegam ao poder judiciário, costumam significar uma absolvição.

Ademais, inúmeras outras previsões do tratado internacional, exigirão que o Congresso Nacional atualize nossa legislação penal, como é o caso da violação de dados, interferências em sistemas e a responsabilidade das pessoas jurídicas, conforme estabelecido no artigo 12º. Esse é um dos pontos mais desafiadores para o nosso ordenamento, porque o dirigente de uma pessoa jurídica passa a responder quando uma pessoa física age sobre autoridade dessa pessoa jurídica, em seu benefício, ou quando faltar supervisão ao controle e realizar um crime. Então, uma situação é quando for uma organização criminosa agindo, outra questão é a uma empresa gerar uma infração de direitos autorais ou pornografia infantil e essas situações puderem responsabilizar o dirigente. Esses são pontos que ainda teremos de tratar[97].

Nesse víes, o artigo 15º, da Convenção prevê a adoção de medidas excepcionais, como ordens de autoridade para investigações, que não necessariamente exigem uma ordem judicial. Essas medidas podem ser aplicadas em situações de flagrante, durante revistas, blitzes, abordagens veiculares, revistas em aeroportos, shows, estádios, e entre outros casos, em que haja uma ameaça extremamente elevada. Quanto aos prazos, o artigo 16º estabelece um período de 90 dias para a preservação de evidências, bem como o artigo 18º deste traz a

---

[96] COLTRO, Rafael Khali. WALDMAN, Ricardo Libel. Criminalidade digital no Brasil: A problemática e a aplicabilidade da convenção de Budapeste. EM TEMPO INSS – 1984 – 7858 DIGITAL.v. 21 n. 01. 2021.

[97] PINHEIRO, Patrícia Peck, **Sobre a adesão do Brasil à Convenção de Budapeste.** Disponível em https://www.telesintese.com.br/peck-sobre-a-adesao-do-brasil-a-convencao-de-budapeste/Acesso: 10. mai. 2023

definição de informação cadastral que é extremamente relevante, assim como o artigo 20 traz obtenção de dados em tempo real, muito importante para termos eficiência no combate ao crime organizado digital. Em contrapartida, no Brasil, possuíamos prazos mais extensos, conforme tipificado pelo Marco Civil da Internet.

Deste modo, a transformação da Convenção de Budapeste em decreto não apenas possibilita a evolução legislativa através do Congresso Nacional para adequações na legislação nacional, mas também habilita a ação imediata dos órgãos administrativos e executivos, como o Ministério da Segurança Pública, com base nos princípios de cooperação e assistência mútua previstos nos artigos 23 e 25, assim como na troca espontânea de informações, conforme estabelecido no artigo 26. Tendo em vista, que são muitos os casos de crimes na Internet ocorridos fora do território nacional, que poderiam ter outro desfecho se fossem apurados no âmbito dos instrumentos de cooperação internacional.

Cabe destacar que as partes envolvidas no intercâmbio de informações, conforme delineado pela Convenção, possuem o direito de solicitar que as informações fornecidas sejam mantidas confidenciais ou sujeitas a condições específicas antes da divulgação. Esta salvaguarda adicional constitui um passo significativo para o Brasil, que tem enfrentado desafios na luta contra o cibercrime, pois já estávamos atrasados nessa área, e que consigamos atuar de forma mais efetiva com a segurança pública no ambiente digital[98].

Dessa forma, com a adesão e à implementação da Convenção de Budapeste, o Brasil ganha mais recursos para combater efetivamente o crime cibernético, protegendo a segurança pública no âmbito digital.

Por conseguinte, o artigo 13 da Convenção orienta seus signatários a tomar as medidas necessárias, levando em consideração as realidades e necessidades específicas de cada país, para assegurar que os atos tipificados como crimes sejam sujeitos a sanções adequadas. Com base nessa perspectiva, André Zaca Furquim, Coordenador-Geral de Cooperação Jurídica Internacional em Matéria Penal do Ministério da Justiça e Segurança Pública (MJSP), acredita que a Convenção de Budapeste pode promover um aumento gradual na cooperação jurídica

---

[98] PINHEIRO, Patrícia Peck, **Sobre a adesão do Brasil à Convenção de Budapeste.** Disponível em https://www.telesintese.com.br/peck-sobre-a-adesao-do-brasil-a-convencao-de-budapeste/. Acesso: 10. mai. 2023

internacional[99]. À medida que as investigações brasileiras requerem cada vez mais provas digitais originadas de outros países, a Convenção pode facilitar e incentivar os investigadores brasileiros a adotar essa estratégia.

Na mesma linha, Carolina Yumi, Diretora do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) do MJSP, enfatiza que a plena implementação da Convenção de Budapeste no Brasil trará benefícios significativos para o país[100]. Esses benefícios incluem o avanço nas normas e políticas relativas ao combate aos crimes cibernéticos e na coleta e preservação de evidências digitais. A Convenção também contribuirá para aprimorar a cooperação internacional nas investigações e esclarecimento de crimes cometidos no ambiente digital, ao mesmo tempo incentivando o Brasil a continuar desenvolvendo seu sistema jurídico e suas políticas face ao avanço da criminalidade no ciberespaço. Logo, isso precisa ser feito mantendo um equilíbrio adequado entre a intensificação da perseguição penal e a proteção dos dados pessoais.

No âmbito jurídico, o documento mencionado articula claramente que, durante emergências, cada Estado signatário tem a prerrogativa de formular pedidos de assistência mútua ou iniciar negociações pertinentes por meio de canais de comunicação acelerados, incluindo *fax* ou e-mail. Esses procedimentos estão especificamente delineados no Artigo 25°, sendo vital ressaltar que a segurança e a autenticação devem ser asseguradas em qualquer comunicação por meio desses canais, exigindo confirmação oficial posterior quando o Estado solicitante assim o requerer. Outro aspecto adicional da Convenção que merece destaque é o conteúdo do Artigo 35°, o qual estipula a constituição de uma rede de assistência composta por Estados membros, no qual essa rede deve estar operacional de maneira contínua - 24 horas por dia, 7 dias por semana - com o intuito de prover assistência imediata em investigações e casos ligados a delitos penais, incluindo a coleta expedita de provas digitais de uma infração penal.

---

[99] MINISTÉRIO DÁ JUSTIÇA DE SEGURANÇA PÚBLICA. **Convenção de Budapeste é promulgada no Brasil.** Disponível em https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso: 15. mai. 2023

[100] MINISTÉRIO DÁ JUSTIÇA DE SEGURANÇA PÚBLICA. **Convenção de Budapeste é promulgada no Brasil.** Disponível em https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso: 15. mai. 2023

l

Com essas novas dinâmicas, como membro da Convenção, o Brasil terá de implementar em sua legislação interna medidas que tipifiquem como crime o acesso intencional e ilegítimo a sistemas informáticos. Essas infrações deverão ser penalizadas com sanções eficazes e proporcionais, contemplando até mesmo penas privativas de liberdade. Assim, a classificação de determinados comportamentos ilícitos na Convenção parece alinhada com o impacto provocado pelos cibercriminosos.

Nesse sentido, se torna pertinente considerar os bens jurídicos tutelados ao estabelecer normas para condutas digitalmente ilícitas, tal como preconizado pela Convenção. O interesse legítimo protegido é difuso e, de acordo com Silva[101], há a necessidade de um direito penal globalizado que busque uma resposta unificada ou, no mínimo, harmoniosa para o crime transnacional, impedindo a criação de paraísos jurídicos para criminosos. Dessa forma, o tratado se mostra abrangente, contemplando a criminalização de comportamentos, padrões para investigação e obtenção de provas eletrônicas e meios de cooperação internacional. Seu maior benefício é a agilidade na troca de dados, e mesmo que a Convenção exija a adesão a certos princípios fundamentais e regras pré-definidas, a sua aplicação é suficientemente flexível para se adaptar à legislação interna de cada país signatário. Logo, seu objetivo primordial é oferecer um norte, ao invés de impor soluções fixas e inflexíveis para os problemas identificados.

Assim, mesmo que fosse visível um progresso modesto na iniciativa do sistema jurídico brasileiro para regular as ações praticadas por meio digitais, tais avanços ainda eram amplamente insuficientes, a Convenção de Budapeste não só permite a tipificação de uma variedade de condutas prejudiciais realizadas por meios digitais, mas também oferece uma estratégia eficaz para lidar com essas questões. Tendo em vista, que como as ações prejudiciais abordadas pela Convenção são perpetradas no ciberespaço, é presumível que o cibercriminoso possa realizar suas ações plenamente, desconsiderando as fronteiras geopolíticas, o que demanda uma uniformização dos sistemas jurídicos.

Compreende-se, que a adesão do Brasil ao tratado parece ser uma solução exímia para a lacuna legislativa presente no contexto cibernético. Outra alternativa seria a criação de um sistema jurídico autônomo, tarefa essa que se mostra

---

[101] SILVA, Ana Laura Rossi. **Cibercrimes: Uma análise sob a perspectiva da aplicação do direito internacional**. Uberlândia - Minas Gerais. UNIVERSIDADE FEDERAL DE UBERLÂNDIA. 2019.

desafiadora, levando em consideração a atual polarização política e ideológica evidente no país, principalmente no legislativo. Assim, a adequação da legislação nacional ao tratado, além de ser viável, trará numerosos benefícios no combate e investigação desses delitos.

CONCLUSÃO

A era digital hodierna, marcado por um constante estado de interconectividade, amplificou nossa susceptibilidade aos cibercrimes, que têm demonstrado uma escala e complexidade cada vez mais alarmantes. A sofisticação e expansão de tais crimes, definidos como atos reprováveis cometidos contra ou por meio do processamento automatizado de dados ou sua transmissão, demonstram como a internet se tornou um novo palco para a prática criminosa. A acessibilidade global da rede desafia fronteiras, tornando a tarefa de rastreamento por autoridades reguladoras cada vez mais desafiadora.

Nesse cenário, se evidencia um descompasso entre as leis e a sociedade moderna, fruto da velocidade com que as transformações tecnológicas ocorrem. A rapidez com que informações são trocadas, combinada com o anonimato proporcionado por esses meios, torna a questão legal ainda mais desafiadora. Como analisado ao longo desta pesquisa, a legislação nacional tem encontrado obstáculos para acompanhar a evolução dos cibercrimes, revelando lacunas que podem ser melhor preenchidas em áreas como proteção de dados, vigilância e cooperação internacional.

Desse modo, identificar cibercriminosos se tornou um desafio mais complexo pela falta de regulamentação que exija dos provedores de acesso e conteúdo a manutenção de registros das atividades na rede de computadores por um período específico, favorecendo o anonimato desses criminosos. Se mostra imprescindível a existência de leis que determinem a conservação desses registros de acesso dos usuários à internet, bem como dos dados referentes as atividades realizadas nesses acessos, por um período adequado e proporcional, tendo em vista que tais dados são necessários para possibilitar a identificação dos responsáveis pelos crimes praticados no ambiente virtual, tornando o anonimato uma exceção, e não a regra, na rede mundial de computadores.

Por conseguinte, os legisladores e estudiosos do direito brasileiro têm se movimentado de forma gradual na construção de normas que tratem do cibercrime, incapazes de acompanhar a evolução da criminalidade virtual. As leis existentes e os projetos de lei em tramitação no Congresso Nacional, não conseguem refletir as exigências atuais de combate ao crime cibernético, necessitando de uma

modernização conceitual e de uma abrangência que ultrapasse a velocidade do avanço tecnológico.

Projetos de lei e alterações legislativas referentes a delicada questão da criminalidade cibernética devem ser criticamente analisados, com propostas de mudanças concretas na redação legislativa, considerando as peculiaridades do ambiente virtual. As dificuldades de investigação, identificação dos criminosos, punição e até a ausência de tipificação desses novos crimes, provocam a falha dos Estados em garantir a proibição de proteção deficiente aos seus cidadãos.

Sob esse panorama, o compromisso do Brasil com a Convenção de Budapeste no combate ao cibercrime, introduz a cooperação indispensável para a perseguição e punição efetiva desses delitos, além das fronteiras nacionais, incentivando a cooperação jurídica internacional. Tal adesão representa um marco importante para a promoção da democracia e a proteção dos direitos humanos, considerando a carência de uma legislação moderna e específica para combater os cibercrimes no Brasil.

Assim sendo, a tecnologia tem um impacto substancial em quase todos os aspectos de nossas vidas, gerando questões complexas e multifacetadas que exigem abordagens inovadoras e adaptativas em termos de legislação e aplicação da lei. Diante disso, o surgimento de cibercrimes sublinha a necessidade de uma abordagem global, coesa e coordenada, uma vez que a natureza transnacional desses crimes ultrapassa as capacidades de qualquer jurisdição individual.

Nesse contexto, embora o Brasil tenha feito alguns avanços em termos de legislação, há uma necessidade premente de adaptar e atualizar as leis e regulamentos existentes para refletir a evolução da tecnologia e da criminalidade online, isso requer uma compreensão profunda das complexidades do ambiente digital, bem como uma abordagem que mantenha um equilíbrio entre a necessidade de proteger os usuários da internet e respeitar as liberdades civis e a intensificação da perseguição penal e a proteção dos dados pessoais.

Assim como o desenvolvimento e a implementação de leis de cibercrime eficazes e justas são desafios que exigem a cooperação entre legisladores, juristas, profissionais de TI e a comunidade em geral, sendo igualmente importante reforçar a conscientização e a educação sobre cibersegurança para prevenir e combater eficazmente os cibercrimes.

Portanto, esta monografia forneceu uma visão sobre o cibercrime, com um foco específico no cenário brasileiro, diante do crescimento exponencial da cibercriminalidade no país. Através da aplicação do método dedutivo, e com o suporte de pesquisas bibliográficas e documentais, foi possível analisar profundamente as características emergentes dos crimes digitais, a evolução da legislação nacional correspondente, assim como as dificuldades de investigação e a problemática do anonimato, bem como a importância e os impactos da adesão do Brasil à Convenção de Budapeste, frente a transformações jurídicas e práticas decorrentes do compromisso com este tratado internacional.

O primeiro capítulo nos permitiu compreender a origem dos cibercrimes e suas diversas tipologias. No segundo capítulo, foi analisado o histórico da legislação nacional em relação à cibercriminalidade, evidenciando a evolução das respostas jurídicas, mas também ressaltando a insuficiência do ordenamento jurídico interno para lidar com os desafios e complexidades inerentes à criminalidade digital. Por conseguinte, o terceiro e último capítulo, se verificou a discussão centrada nas normas internas, na problemática do anonimato e na análise das transformações jurídicas e práticas após a adesão à Convenção de Budapeste, mostrando a relevância deste tratado para aprimorar as capacidades do Brasil de enfrentar a cibercriminalidade.

Fica evidente, portanto, que a adesão do Brasil à Convenção de Budapeste representa um passo significativo em direção a uma abordagem mais robusta, abrangente e atualizada no combate à cibercriminalidade. Com isso, esta adesão não apenas fornece um marco legal internacionalmente reconhecido, mas também promove a cooperação internacional e oferece diretrizes valiosas para a criação e adaptação de leis nacionais. Assim, com a implementação da Convenção de Budapeste, o Brasil ganha mais recursos para combater efetivamente o crime cibernético, protegendo a segurança pública no âmbito digital. Todavia, se mostra crucial enfatizar que a adesão a Convenção é apenas parte da solução, de modo que se vivifica fundamental que o Brasil continue a desenvolver uma legislação interna robusta e adequada que complemente as disposições do tratado e que esteja apta a responder de modo eficaz às mudanças dinâmicas do cenário da cibercriminalidade. Logo, a ratificação da Convenção de Budapeste marca um ponto determinante na luta do Brasil contra a cibercriminalidade, abrindo caminho para uma abordagem mais eficiente e atualizada no combate aos delitos 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://sistemas.uft.edu.br/periodicos/index.php/direito/article/view/4171#:~:text=O%20presente%20artigo%20busca%20compreender,Leis%20Penais%20regulando%20esse%20crime..

ARAUJO, Nádia de. **A importância da cooperação jurídica internacional para a atuação do estado brasileiro no plano interno e internacional.** Manual de Cooperação Jurídica Internacional e Recuperação de Ativos. Brasília: Ministério da Justiça, 2012.

BARRETO, Alesandro Gonçalves. SANTOS, Hericson dos. Deep Web: **investigação no submundo da internet.** 1. Ed. Rio de Janeiro: Editora Brasport, 2019. BRASIL. Supremo Tribunal Federal. Informativo STF n° 286/2002. Disponível em http://www.stf.jus.br//arquivo/informativo/documento/informativo286.htm..

BECK, Ulrich. **Sociedade de risco: rumo a uma outra modernidade.** Tradução de Sebastião Nascimento. São Paulo: Ed. 34, 2010.

_____. **Sociedade de risco mundial:** em busca da segurança perdida. Edições 70, 2015.

BITTAR, Carlos Alberto. **Os Direitos da Personalidade.** Rio de Janeiro: Forense Universitária, 1989.

BRANCO, Paulo Gustavo Gonet; COELHO, Inocêncio Mártires; MENDES, Gilmar Ferreira. **Curso de Direito Constitucional**. 4ª. ed. São Paulo: Saraiva, 2008. p. 404.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. Supremo Tribunal Federal. **Informativo STF n° 393/2005.** Disponível em http://www.stf.jus.br/arquivo/informativo/documento/informativo393.htm.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário n° 125.556/PR**. Disponível em http://www.stf.jus.br/. Acesso em 06 de setembro de 2020. BRASIL. Supremo Tribunal Federal. MS 24.405-4-DF. Rel. Min. Carlos Velloso. Disponível em http://www.stf.jus.br/.

BRASIL. Supremo Tribunal Federal. **HC 82.424. Rel. p/ o ac.** Min. Presidente Maurício Corrêa. Disponível em http://www2.stf.jus.br/portalStfInternacional/cms/verConteudo.php?sigla=portalStfJurisprudencia_pt_br&idConteudo=185077&modo=cms.

BRASIL. Supremo Tribunal Federal. **Ação Direita de Inconstitucionalidade n° 1969- 2007**. Rel. Min. Ricardo Lewandosvik. Disponível em http://www.stf.jus.br/. Acesso em 08 de setembro de 2020. Brasil adere à Convenção de Budapeste e se posiciona contra crimes cibernéticos. Disponível em https://diariodoturismo.com.br/brasil-adere-a-convencao-de-budapestee-se-posiciona-contra-crimes/.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm.

BRASIL. DECRETO 75.699, DE 6 DE MAIO DE 1975. Promulga a **Convenção de Berna para a Proteção das Obras Literárias e Artísticas,** de 9 de setembro de 1886, revista em Paris, a 24 de julho de 1971. Disponível em https://www.planalto.gov.br/ccivil_03/decreto/1970-1979/d75699.htm. Acesso 25.maio.2023

BRASIL. **Lei 8.069, de 13 jul. 1990.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm.

BRASIL. **Lei 9.279, de 14 de maio de 1996.** Regula direitos e obrigações relativos à propriedade industrial. Disponível em https://www.planalto.gov.br/ccivil_03/leis/l9279.htm Acesso 20.mai.2023

BRASIL. **Lei 9.296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm.

BRASIL. **Lei 9.610, de 19 de fevereiro de 1998.** Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Disponível em https://www.planalto.gov.br/ccivil_03/leis/l9610.htm Acesso. 20.mai.2023

BRASIL. **Lei nº 9.983, de 14 de julho de 2000.** Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9983.htm.

BRASIL. **Lei 10.695, de 01 de julho de 2003.** Altera e acresce parágrafo ao art. 184 e dá nova redação ao art. 186 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal, alterado pelas Leis nos 6.895, de 17 de dezembro de 1980, e 8.635, de 16 de março de 1993, revoga o art. 185 do Decreto-Lei no 2.848, de 1940, e acrescenta dispositivos ao Decreto-Lei no 3.689, de 3 de outubro de 1941 – Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/l10.695.htm.

BRASIL. **Lei 11.829, de 25 de novembro de 2008.** Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm.

BRASIL. **Lei 12.735, de 30 nov. 2012.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm.

BRASIL. **Lei 12.737, de 30 nov. 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.

BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm; Acesso em 27.maio.2023

BRASIL. **Lei 13.869, de 5 de setembro de 2019.** Dispõe sobre os crimes de abuso de autoridade; altera a Lei nº 7.960, de 21 de dezembro de 1989, a Lei nº 9.296, de 24 de julho de 1996, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 8.906, de 4 de julho de 1994; e revoga a Lei nº 4.898, de 9 de dezembro de 1965, e dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13869.htm#art45.

BRASIL. **Lei nº 13.964 de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm.

BRASIL**.Lei 14.155, de 27 de maio de 2021**. Aperfeiçoa a legislação penal e processual penal. Disponível em http://https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso 01.jun.2023

BRASIL. **Marco civil da internet:** Lei n. 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 2. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2015.

BRANCO, Paulo Gustavo Gonet. COELHO, Inocêncio Mártires. MENDES, Gilmar Ferreira. Curso de Direito Constitucional. 4ª. ed. São Paulo: Saraiva, 2008. 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&revist a_caderno=17.

CAVALCANTE. Márcio André Lopes. Lei 14.155/2021: **promove alterações nos crimes de violação de dispositivo informático, furto e estelionato** https://www.dizerodireito.com.br/2021/05/lei-141552021-promove-alteracoes-nos.html. Acesso 3. jun.2023

CANUTO, Luiz Cláudio. CPI **constata dificuldade em rastrear e punir crimes de internet.** Disponível em https://www.camara.leg.br/noticias/467819-cpi-constatadificuldade-em-rastrear-e-punir-crimes-de-internet/.

CARBONI, Guilherme C. **A Lei nº 10.695/03 e seu impacto no Direito Autoral Brasileiro. 2003.** Disponível em https://www.migalhas.com.br/impacto-no-direito-autoral-brasileiro.

CARDOSO, Luiz Eduardo; FALAVIGNO, Chiavelli Facenda. **Do Pacote Anticrime ao Código Penal**: uma análise comparativa da disciplina da perda alargada na Lei n. 13.964/2019. 2020. No prelo.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação.** Âmbito jurídico, 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-umareflexao-sobre-o-problema-na-tipificacao/.

CARVALHO, Paulo Sergio de. **Noções Gerais de Direitos autorais**. Escola Nacional de Administração Pública - ENAP. 2014.

CENTRO DE PREVENÇÃO, TRTAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO. **Abuso de Sítio Web.** Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros/abuso-de-sitio-web.

CENTRO DE PREVENÇÃO, TRTAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO. **Incidentes.** Disponível em: https://www.gov.br/ctir/ptbr/assuntos/ctir-gov-em-numeros/incidentes .

CERT.br. **Cartilha de Segurança para Internet.** Versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 18. abril. 2023

CERT.br. **Incidentes reportados ao CERT.br:** Janeiro a Junho de 2020. 2020. Disponível em: https://www.cert.br/stats/incidentes/2020-jan-jun/fraude.html. Acesso em: 18. abril. 2023

CERT.br. **Vazamento de Dados.** 2021. Disponível em: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf.

CHADD, Katie. **The history of cybersecurity.** Avast, 2020. Disponível em: https://blog.avast.com/history-of-cybersecurity-avast.

CISO Advisor. S**TJ comunica superação do incidente cibernético com ransomware.** 2020. Disponível em: https://www.cisoadvisor.com.br/stj-comunica-superacao-do-incidentecibernetico-com-ransomware/.

CONVENÇÃO de Budapeste. 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacaotematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-dobrasil/docs_legislacao/convencao_cibercrime.pdf.

COUTINHO, Isadora Caroline Coelho. **Pedofilia na era digital.** Ambito Juridico. 2011. Disponível em: https://ambitojuridico.com.br/edicoes/revista-94/pedofilia-na-era-digital/amp/.

COMISSÃO EUROPEIA. Proteção de dados nas instituições e outros organismos da UE. Disponível em https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt#:~:text=O%20Regulamento%20(UE)%202018%2F,Dados%20na%20Aplica%C3%A7%C3%A3o%20da%20Lei. Acesso em 28.maio.2023

CRESPO, Marcelo. **Ransonware e sua tipificação no Brasil.** Canal Ciências Criminais. Disponível em: https://canalcienciascriminais.jusbrasil.com.br/artigos/249364352/ransonware-e-suatipificacao-nobrasil#:~:text=A%20pr%C3%A1tica%20do%20ransonware%20%C3%A9,se%20nota%20pel
a%20reda%C3%A7%C3%A3o%20t%C3%ADpica).&text=Ent%C3%A3o%20um%20crime%20grave%20como,do%20modus%20operandi%20do%20criminoso.

CUNHA, Rogério Sanches. Pacote Anticrime: Lei n. 13.964/19 - **Comentários às alterações no CP, CPP e LEP.** Salvador: Juspodivm, 2020b.

CRUZ, Diego; RODRIGUES, Juliana. **Crimes cibernéticos e a falsa sensação de impunidade.** Revista científica eletrônica do curso de direito. 13ª Ed. Disponível em

http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf.

Declaração Universal dos Direitos do Homem. Disponível em http://pfdc.pgr.mpf.mp.br/atuacao-econteudos-de-apoio/legislacao/direitos-humanos/declar_dir_homem.pdf.

DIANA, Daniela. **História da internet.** Disponível em https://www.todamateria.com.br/historia-dainternet/. Acesso em 14 abril. 2023

DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indiciosda-autoria-e-prova-da-materialidade. Acesso 05. mai. 2023

FUNDAÇÃO Escola Superior do Ministério Público. **Lei Carolina Dieckmann:** Você sabe o que essa lei representa? 2021. Disponível em: https://fmp.edu.br/lei-carolina-dieckmannvoce-sabe-o-que-essa-lei-representa/.

FUTURE. **Brasil: um dos líderes em controle de botnet.** 2017. Disponível em: https://www.future.com.br/blog/brasil-um-dos-lideres-em-controle-de-botnet/.

GATEFY. **BEC e phishing ainda continuam na moda, diz o relatório do FBI**. 2021. Disponível em: https://gatefy.com/pt-br/blog/bec-phishing-continuam-moda-diz-relatoriofbi/.

GIACCHETTA, André Zonaro. **A nova arma no combate à pirataria - a Lei Nº 10.695, de 2.7.2003.** Migalhas, 2003. Disponível em: https://www.migalhas.com.br/depeso/2275/a-novaarma-no-combate-a-pirataria---a-lei--n---10-695---de-2-7-2003.

GIDDENS, Anthony. **As consequências da modernidade.** São Paulo: Editora UNESP, 1991

GUARAGNI, Fábio André. RIOS, Rodrigo Sanchez. **Novas tendências de combate aos crimes cibernéticos: cooperação internacional e perspectivas na realidade brasileira contemporânea.** Revista de Estudos
Criminais. Porto Alegre, v. 18, n. 73. p. 181. 2019.

GUARAGNI, Fábio André. RIOS, Rodrigo Sanchez. **Novas tendências de combate aos crimes cibernéticos:** cooperação internacional e perspectivas na realidade brasileira contemporânea. Revista de Estudos Criminais. Porto Alegre, v. 18, n. 73. p. 181. 2019.

INTERPOL. **Cybercrime: Covid-19 Impact.** 2020. Disponível em: https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

JESUS, Damásio De. ARAS, Vladmir. Crimes de informática: **Uma nova criminalidade.** Disponível em .https://jus.com.br/artigos/2250/crimes-de-informática. Acesso em 17 de abril. 2023

JUNIOR, Júlio Cesar Alexandre. **Cibercrime: um estudo acerca do conceito de crimes informáticos**. Revista Eletrônica da Faculdade de Direito de Franca. Disponível em . Acesso em

https://www.revista.direitofranca.br/index.php/refdf/article/view/602#:~:text=Cibercrime%20est%C3%A1%20associado%20ao%20%E2%80%9Cfen%C3%B3meno,12). Acesso. 10 abril. 2023

KASPERSKY. **Ciberataques crescem 23% no Brasil em 2021**. 2021. Disponível em: https://www.kaspersky.com.br/blog/panorama-ciberameacas-brasil-2021-pesquisa/18020/.

KAMINSKI, Omar. **Conheça o Tratado Internacional contra crimes na Internet.** Revista Consultor Jurídico. Disponível em . https://www.conjur.com.br/2001-nov-4/convencao_lanca_tratado_internacional_cibercrimes.

LEON, Lucas Pordeus. **Brasil tem 152 milhões de pessoas com acesso à internet.** AgênciaBrasil, Brasília, 2021. Disponível em: Brasil tem 152 milhões de pessoas com acesso à internet | Agência Brasil (ebc.com.br).

LIMA, Renato Brasileiro de. **Pacote Anticrime:** Comentários à Lei 13.964/2019 artigo por artigo. Salvador: Juspodivm, 2020. Acesso. 29.maio.2023

LOURENÇO, Gabriel D. **Ataque da Mão Fantasma: novo golpe brasileiro rouba a vítima diante dos próprios olhos.** Olhar Digital, 2021. Disponível em: https://olhardigital.com.br/2021/08/31/seguranca/ataque-da-mao-fantasma/ .

NASCIMENTO, Talles Leandro Ramos. Crimes cibernéticos. Conteúdo Jurídico. Disponível em . https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em 23. mai. 2023

MATIAS, Juliana. **Crimes digitais: 'Atual legislação vive de puxadinhos', diz desembargadora do TJSP.** Disponível em https://www.jota.info/jotinhas/crimes-digitais-atual-legislacao-vive-de-puxadinhos-diz-desembargadora-do-tjsp-09062022 26.mai.2023

MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Borges. **Os Crimes Cibernéticos no Ordenamento Jurídico Brasileiro e a Necessidade de Legislação Específica.** Disponível em http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e a-necessidade-de-legislacao-especifica-2. Acesso: 14 de abr..2023

MENDONÇA, Cláudia da Silva. **Guerra Cibernética: Desafios de uma Nova Fronteira.** Rio de Janeiro, 2014.

MILAGRE, José Antônio. **Lei Azeredo, AI-5 digital e a cultura do contra. Uma visão pessoal sobre o manifesto contra a Lei de Crimes de Informática**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 14, n. 2216, 26 jul. 2009. Disponível em: https://jus.com.br/artigos/13211.

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

MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO.. **Marco Civil da Internet: Perspectivas gerais e apontamentos críticos.** São Paulo.

MINISTÉRIOS DAS RELAÇÕES EXTERIORES. **Processo de adesão à Convenção de Budapeste** -Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública. Disponível emhttp://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-

MORAES, Alexandre de. **Direito constitucional.** 15. Ed. – São Paulo: Atlas, 2004. p. 74

MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico. Disponível em https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/. Acesso: 2.jun.2023.

PINHEIRO, Patrícia Peck, **Sobre a adesão do Brasil à Convenção de Budapeste**. Disponível em https://www.telesintese.com.br/peck-sobre-a-adesao-do-brasil-a-convencao-de-budapeste/

PINHEIRO, Patrícia Peck, Direito digital. 6.ed., atual. e ampl. São Paulo: Saraiva, 2016.

PROPRIEDADE INTELECTUAL, **Estratégia Nacional de Propriedade Intelectual.** 2021. Disponível em https://www.gov.br/pt-br/propriedade-intelectual/estrategia-nacional-de-propriedade-intelectual Acesso 28.maio.2023

RAINS, Tim. **CybersecurityThreats, Malware Trends, andStrategies: mitigateexploits, malware, phishingandother social engineeringattacks**. Birmingham: PacktPublishing Ltd, 2020. 429 p.

ROVER, Tadeu. **Violência virtual: internet facilita crimes e dificulta investigação, estimulando a impunidade.** Disponível em https://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais..

ROMANO, Rogério Tadeu. CONVENÇÃO DE BUDAPESTE E CIBERCRIMES. Disponível em. https://jus.com.br/artigos/72969/convencao-de-budapeste-e-cibercrimes. Acesso em 5. jun. 2023.

SAFERNET, Brasil - Protegendo os Direitos Humanos na Sociedade da Informação. **Parcerias com o MPF.** Disponível em https://www.safernet.org.br/site/institucional/parcerias/mpf. Acesso 01 jun. 2023

SANCHES, Ademir Gasques. ANGELO, Ana Elisa de. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil

SANTOS, Elaine Gomes dos. RIBEIRO, Raisa Duarte da Silva. **Restrições à liberdade de expressão e crimes cibernéticos: a tutela penal do discurso de ódio nas redes sociais.** Revista dos Tribunais. vol. 997. ano 107. p. 527. São Paulo: Editora RT. novembro 2018.

Secretaria Geral da Presidência da República. **Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética**. Disponível em

https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica. Acesso 9.maio.2023

SEGURANÇA,Justiça. **A Convenção de Budapeste é promulgada no Brasil**. Disponível em https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil.

SENADO. C**ombate ao cibercrime é urgente, afirmam especialistas na CCT.** Disponível https://www12.senado.leg.br/noticias/materias/2021/12/15/combate-ao-cibercrime-e-urgente-afirmam-especialistas-na-cct.

SENADO. **Comissão de Relações Exteriores e Defesa Nacional.** Disponível https://www25.senado.leg.br/web/atividade/notas-taquigraficas/-/notas/r/10148 Acesso. 18. mai.2023

SENADO FEDERAL. **Projeto de Lei n. 6.341, de 2019.** 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/140099.

SEGURANÇA PÚBLICA, **Governo Federal lança Plano Tático de Combate a Crimes Cibernéticos.** 2022. Disponível em https://www.gov.br/pt-br/noticias/justica-e-seguranca/2022/03/governo-federal-lanca-plano-tatico-de-combate-a-crimes-ciberneticos. Acesso. 18. mai.2023

SILVA, Rita de Cássia Lopes. **Direito Penal e Sistema Informático**. Revista dos Tribunais, 2003.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em. https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras. Acesso 02.jun.2023

STEINBERG, Joseph. **Cibersegurança para leigos**. 1 ed. Rio de Janeiro: Alta Books, 2021.

Symantec; Organizações dos Estados Americanos. Relatório '**Tendências de Cibersegurança na América Latina e no Caribe**". 2014. Disponível em https://www.broadcom.com/404-symantec?sourceURL=http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc-annex.pdf?

TRUZZI, Gisele. **Direitos autorais e internet: como usar conteúdo de terceiros sem problemas**. Disponível em https://www.conjur.com.br/2020-ago-24/gisele-truzzi-direitos-autorais-internet. Acesso 20.mai.2023

VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 236.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes Cibernéticos: Ameaças e procedimentos de investigação**. 3 ed. Rio de Janeiro: Brasport, 2021.

WINDER, Davey. **This 20-Year-Old Virus Infected 50 Million Windows Computers In 10 Days:** Why The ILOVEYOU Pandemic Matters In 2020. FORBES, 2020. Disponível em: https://www.forbes.com/sites/daveywinder/2020/05/04/this-20-year-old-virus-infected-50-

million-windows-computers-in-10-days-why-the-iloveyou-pandemic-matters-in2020/?sh=10a
a7f8b3c7c.